

G DATA NotebookSecurity

Bedienung

Inhalt

Allgemeines	7
Ein paar Worte vorab	7
G DATA ServiceCenter	8
Tipps zur Virenprophylaxe	9
Systemvoraussetzungen	11
 Installation.....	 12
Installationsvorbereitung	12
BootScan	12
Installationsvorgang	14
 Beim ersten Start	 22
Internet Update	22
Virenprüfung	24
 Allgemeine Programminformationen	 27
Bedienung der Software	27
Windows Kontextmenü	27
Shredder	28
Security-Symbol	28
SecurityLock	29
AntiVirus Boot-CD erstellen	31
 SecurityCenter.....	 32
 AntiVirus	 33
Bedienung der Software	33
Menüleiste	34
Programmbereiche	34
Optionen	50

Firewall.....	68
Erste Schritte	68
Bedienung der Software	69
Menüleiste	70
Programmbereiche	71
Optionen	81
Regeln erstellen	89
 AntiSpam	 100
Die Bedienung von AntiSpam	100
Programmbereiche	101
Optionen	109
Spam-Filter	112
 Webfilter	 120
Bedienung des Webfilters	120
Webfilter-Symboleiste im Internet Explorer	122
Programmbereiche	124
 Kindersicherung.....	 129
Die Bedienung der Software	129
Programmbereiche	130
Optionen	141
 Tuner.....	 143
Bedienung des Tuners	143
Programmbereiche	148
 Backup.....	 164
Die Bedienung der Software	164
Programmbereiche	166

TopSecret	181
Einführung	181
Erster Programmstart	183
Programmaufbau	188
Safes	194
 Anhang	 212
Lizenzvereinbarungen	212
Virengeschichte	213
Glossar	219
Virenkategorien	255
Index	261

Allgemeines

■ Ein paar Worte vorab

Notebooks brauchen mehr Schutz als Desktop-PCs durch ein erhöhtes Schädens- und Verlustrisiko. **G DATA NotebookSecurity** bietet einen einmaligen Umfang speziell für Notebooks und kombiniert **G DATA InternetSecurity** mit Backup, Verschlüsselung, Notebook-Schloss und einer optionalen Notebook-Versicherung.

G DATA AntiVirus

- DoubleScan & Outbreakshield: Preisgekrönte Virenerkennung
- Virenblocker für Mails, HTTP und Instant Messaging

G DATA Personal Firewall

- Preisgekrönter Schutz vor Attacken
- Games-Optimierung: Autopilot für transparenten Schutz

NEU: G DATA TopSecret

- Datensafe (virtuelles Laufwerk) zum Verschlüsseln Ihrer Daten
- Echtzeit-Verschlüsselung mit 5 Algorithmen (AES, RC6 etc.)
- Unterstützt Fingerprint-Leser und Sicherheits-Zertifikate

NEU: G DATA SecurityLock

- Effektiver Hardware-Schutz für alle Notebooks (m. Lock-Slot)
- Stahlkabel mit Schloss zum Befestigen an Tischbeinen o.ä.

G DATA Backup

- Automatische Daten-Backups, einfache Wiederherstellung
- Backup auf Datenträger oder online (inkl. 1 GB Speicher)

G DATA AntiSpam / AntiPhishing

- Effektiver Schutz vor Spammails und Phishing-Attacken

Weitere Module

- Security-Tuning, Kindersicherung, Spurenlöscher, Datenschredder, Bannerblocker
- Erkennungs-Updates im Minutentakt, Software-Updates und -Upgrades für ein Jahr enthalten

■ G DATA ServiceCenter

Das G DATA ServiceCenter steht registrierten Kunden zur Verfügung. Es hilft Ihnen bei allen Problemen, die im Zusammenhang mit dem Produkt auftreten per Telefon, Telefax oder E-Mail. Die Kontaktdaten des ServiceCenters erhalten Sie von uns unmittelbar nach der Anmeldung am Update-Server.

■ Sie finden die dazu notwendige **Registriernummer** auf der Rückseite des Bedienungshandbuches. Wenn Sie die Software online gekauft haben, erhalten Sie die Registrierungsnummer online übermittelt.

Während der Installation der Software haben Sie die Möglichkeit, sich zu direkt online zu registrieren. Wahlweise können Sie sich aber auch jederzeit nach der Installation registrieren lassen, indem Sie den Programmpunkt „**Internet-Update**“ aufrufen. Sollten Sie bereits vor der Anmeldung eine telefonische Hilfestellung benötigen, können Ihnen unsere Mitarbeiter im ServiceCenter telefonisch weiterhelfen. Bitte halten Sie für das Gespräch Ihre Kundendaten (Kundennummer oder Registrierungsnummer o.ä.) sowie Zettel und Stift bereit!

Deutschland: 0180 555 48 40

(14 Cent/Minute aus dem deutschen Festnetz. Aus dem Mobilfunknetz können ggf. abweichende Preise gelten.)

Österreich: + 49 (0) 180 555 48 40

(14 Cent/Minute aus dem österreichischen Festnetz. Aus dem Mobilfunknetz können ggf. abweichende Preise gelten.)

Schweiz: + 49 (0) 180 555 48 40

(14 Cent/Minute aus dem Festnetz der Schweiz. Aus dem Mobilfunknetz können ggf. abweichende Preise gelten.)

Prüfen Sie vor jedem Gespräch mit der Hotline bitte, mit welcher Soft- und Hardware Ihr Computersystem ausgestattet ist. Bitte richten Sie es für die Beratung möglichst so ein, das Telefon in der Nähe Ihres angeschalteten Rechners zu haben. Die Software sollte zu diesem Zeitpunkt auf Ihrem Rechner installiert sein.

Bei vielen Problemen können Ihnen oft bereits Hilfetexte und Handbuch weiterhelfen. Bitte versuchen Sie zunächst hier eine Antwort auf Ihre Fragen zu finden. Viele Fragen sind auch bereits in der Online-Datenbank für häufig gestellte Fragen (FAQ) beantwortet worden, die Sie im Support-Bereich der G DATA-Homepage aufrufen können: www.gdata.de

■ G DATA AntiVirus Unternehmenslösungen

Professionellen Virenschutz mit der preisgekrönten DoubleScan-Technologie gibt es auch für **Netzwerke**. Hocheffizient, vollautomatisch und fernsteuerbar. Ob als **client/server-basierte Komplettausrüstung** des Netzwerkes oder als serverunabhängiges **Gateway für Ihre Mailkorrespondenz** - G DATA bietet 100% Virenschutz für beliebige Netzwerke jeder Größe. Informieren Sie sich einfach unverbindlich bei unserem Business-Vertrieb während der üblichen Geschäftszeiten unter:

Tel.: +49 (0)234 / 9762-170

Fax: +49 (0)234 / 9762-298

E-Mail: b-vertrieb@gdata.de

■ *Selbstverständlich wird unser Business-Vertrieb Ihre Anfragen bestmöglich bearbeiten und Sie individuell beraten. Haben Sie bitte Verständnis dafür, dass technische Fragen zur vorliegenden Software nur über unser ServiceCenter bearbeitet werden können.*

■ Tipps zur Virenprophylaxe

Obwohl die G DATA Antiviren-Software auf Basis international renommierter Virenerkennungstechnologien nicht nur bekannte Viren entdeckt und beseitigt, sondern mit Hilfe der heuristischen Analyse auch bis dato unbekannte Schadprogramme anhand Ihrer besonderen Spezifika erkennt, ist es fraglos besser, einen Virenbefall von vornherein auszuschließen bzw. die Möglichkeiten dafür zu minimieren. Dazu sollten sowohl bei Einzelplatzrechnern, als auch in Netzwerken einige Sicherheitsvorkehrungen getroffen werden, die nicht viel Mühe kosten, die Sicherheit Ihres Systems und Ihrer Daten jedoch merklich erhöhen.

■ Original-Software verwenden

Auch wenn in sehr seltenen Fällen auch die Datenträger von Original-Software virenverseucht sein können, ist die Wahrscheinlichkeit einer Vireninfiltration durch Raubkopien oder Kopien auf wiederbeschreibbaren Datenträgern erheblich höher. Benutzen Sie deshalb nur Original-Software. Seien Sie außerdem beim Download von Software aus dem Internet äußerst kritisch und verwenden Sie nur Software die Sie auch wirklich benötigen und deren Herkunft Ihnen vertrauenswürdig erscheint. Öffnen Sie niemals Dateien, die Ihnen per E-Mail von Unbekannten zugeschickt wurden oder die überraschend von Freunden, Kollegen oder Bekannten kommen. Vergewissern Sie sich vorher lieber durch eine Nachfrage an betreffender Stelle, ob Sie die jeweilige Anwendung gefahrlos starten können oder nicht.

■ Festlegen von Verhaltensmaßregeln

Gerade wenn Computer von mehreren Personen genutzt werden, ist es sinnvoll sich auf gemeinsame Verhaltensmaßregeln zu verständigen, die die Systemsicherheit erhöhen helfen:

- Gerade im Hinblick auf das Internet sollten Anwender dahingehend geschult werden, keine Programme aus dem Internet herunterzuladen oder unkritisch Dateianlagen von E-Mails auszuführen.
- Wirken Sie darauf hin, dass bei Virenbefall Gegenmaßnahmen nur von kompetenten Personen durchgeführt werden. So ist es in vielen Fällen gar nicht nötig, infizierte Dateien zu löschen, da sie repariert werden können. Eine entsprechende Einweisung von Mitbenutzern Ihres Computers, sich bei Virenbefall grundsätzlich an den Administrator des Systems zu wenden, kann Ärger vermeiden, zumal die Virenbekämpfung auf diese Weise sinnvoll koordiniert wird.
- Um HTML-Viren keine unnötige Angriffsfläche zu bieten, ist es empfehlenswert, die Vorschaufunktion in E-Mailprogrammen auszuschalten, die in dieser Hinsicht einen möglichen Infektionsweg eröffnet.
- Auf Kettenbriefe und SPAM-Mail sollte grundsätzlich nicht geantwortet werden. Selbst wenn solche E-Mails keinen Virus enthalten sollten, belastet Ihre unerwünschte Weiterleitung den Datenfluss im Internet erheblich.
- Sollte der Anwender einen Virenverdacht haben, z.B. weil eine neu installierte Software nicht das tut, was erwartet wurde oder eine Fehlermeldung auswerfen, sollte er noch vor dem Herunterfahren des Rechners den Administrator mit einem Virencheck beauftragen, da z.B. einige Trojanische Pferde Löschbefehle erst beim nächsten Neustart des Rechners ausführen und auf diese Weise vorher einfacher zu entdecken und bekämpfen sind.
- Wichtig ist es ebenso, darauf hinzuweisen, dass das Ausführen von Makro-Befehlen der Windows-Office-Anwendungen deaktiviert wird, da gerade dadurch die größten wirtschaftlichen Schäden entstehen. Im Hinblick darauf sollte man in Microsoft Office-Produkten unbedingt den Makrovirus-Schutz einschalten. Generell gibt es nur sehr wenige Dateien, die wirklich notwendige Makros enthalten.
- Schließlich sollte es zur regelmäßigen Routine werden, die aktuellen Patches von Microsoft einzuspielen, da diese oftmals neu entdeckte Sicherheitslücken von Windows schließen, bevor ein Virenprogrammierer überhaupt auf die Idee kommt, diese für neue Schadroutinen auszunutzen.

■ Änderung der BIOS-Startreihenfolge

Viele Virenprobleme lassen sich durch die Boot-Up-Sequenz „**C:**, **A:**“ vermeiden. Diese BIOS-Einstellung lässt sich im CMOS-Setup-Menü (gedrückte **Entf**-Taste beim Booten Ihres Rechners) ändern. Auf diese Weise bootet Ihr Computer nicht von oftmals versehentlich eingelegten CD-ROMs oder DVD-Roms, sondern von der Festplatte, was zumindest eine Infektion mit Bootviren erschwert.

■ Informationen zu Viren

Wenn Sie sich eingehend mit der Virenproblematik beschäftigen möchten, finden Sie viele interessante Artikel und Informationen im G DATA Online-Virenlexikon unter www.antiviruslab.com.

■ Systemvoraussetzungen

Zur problemlosen Verwendung der Software benötigt Ihr Computersystem folgende Mindestvoraussetzungen:

- PC mit Windows Vista, Windows XP (ab SP 2) oder Windows® 2000 (ab SP 4)
- Ab 256 MB RAM Arbeitsspeicher, Internet-Zugang, MS InternetExplorer 5.5 oder höher

■ **Achtung: Das Programm-Modul „TopSecret“ steht Ihnen nur auf 32-Bit-Systemen zur Verfügung. Auf 64-Bit-Systemen ist eine Installation nicht möglich.**

Installation

■ Installationsvorbereitung

Führen Sie eine Installation nur auf einem virenfreien System durch. Sollten Sie sich nicht sicher sein, ob Ihr System virenfrei ist, führen Sie bitte vor der Installation der G DATA-Software einen BootScan durch, wie er im folgenden Kapitel beschrieben ist.

■ Sollten Sie schon **andere Antivirensoftware** auf Ihrem Rechner haben, bevor Sie die G DATA-Software installieren (z.B. die Programme anderer Virenhersteller oder auch kostenlose Virenschutzsoftware aus dem Internet), sollten Sie diese **UNBEDINGT VOR DER INSTALLATION der G DATA-Software deinstallieren** und dann den Rechner neu starten. Die besonderen Eigenschaften einer Antivirensoftware führen leider immer dazu, dass ein Betrieb mehrerer Antivirenprodukte erhebliche Probleme mit sich bringt.

■ Es ist ebenfalls empfehlenswert, **Vorgängerversionen der G DATA Antiviren-Software** vor der Installation der neuen G DATA Antiviren-Software zu deinstallieren. Wenn Sie bei der Deinstallation die Option „**Programmeinstellungen und Protokolle beibehalten**“ wählen, übernimmt die neu installierte G DATA Antiviren-Software die Einstellungen der Vorgängerversion.

Schließen Sie bitte alle anderen Programme, bevor Sie mit der Installation der G DATA Antiviren-Software beginnen. Es kann zu Fehlfunktionen oder einem Abbruch der Installation führen, falls z.B. Programme geöffnet sind, die auf Daten zugreifen, die zur Installation benötigt werden.

■ BootScan

Führen Sie bitte unbedingt **vor der Installation** der Software einen **BootScan** mit der BootCD durch! Diese prüft, ob Ihr System bereits von Viren befallen ist. Versäumen Sie es, den BootScan durchzuführen, kann es Ihnen passieren, dass beispielsweise Stealth-Viren den Virenschutz umgehen und erst später oder gar nicht auffallen. Eine korrekte Installation der G DATA Antiviren-Software mit vorhergehendem BootScan sähe folgendermaßen aus:

1. **Legen Sie die G DATA Software-CD in das CD-ROM-Laufwerk Ihres Computers.**
2. **Schalten Sie nun Ihren Computer für mindestens fünf Sekunden aus:** Dies ist nötig, da manche Stealth-Viren in der Lage sind, sich gegen einen Warmstart bzw. ein Reset zu schützen.

3. **Schalten Sie nun Ihren Computer wieder ein:** Ihr Computer fährt nun nicht mit dem Standard-Windows-Betriebssystem hoch, sondern es erscheint die Programmoberfläche einer speziellen G DATA Antiviren-Software-Version, die Sie dabei unterstützt, schon vorhandene Viren von Ihrem Computer zu entfernen. Sollte Ihr Computer nicht von CD-ROM booten, müssen Sie Ihren Computer erst so einstellen, dass er von CD-ROM bootet.
4. **Nutzen Sie die G DATA Antiviren-Software auf der BootCD, um Ihren Computer auf Viren zu überprüfen und diese gegebenenfalls zu entfernen:** Erläuterungen zur Verwendung des BootScans finden Sie in der Online-Hilfe, die Ihnen beim Starten der BootCD zur Verfügung steht.
5. **Nehmen Sie die G DATA Software-CD aus dem CD-ROM-Laufwerk Ihres Computers heraus.**
6. **Schalten Sie erneut Ihren Computer aus und wieder an:** Nun startet Ihr Computer wieder mit Ihrem Standard-Windows-Betriebssystem und Sie haben die Gewähr, die reguläre G DATA Antiviren-Software auf einem virenfreien System installieren zu können.
7. **Legen Sie nun die G DATA Software-CD wieder in Ihr CD-ROM-Laufwerk ein.**
8. **Führen Sie nun die eigentliche Installation der G DATA Antiviren-Software durch:** Die eigentliche Installation der G DATA Antiviren-Software wird Ihnen in den folgenden [Kapiteln](#) ausführlich erläutert.

■ **Was ist eine BootCD?**

Eine BootCD ist eine CD-ROM, die „bootfähig“ ist, über die also ein eigenes Betriebssystem direkt gestartet werden kann. Der Computer startet dann nach dem Einschalten also nicht mit dem auf der Festplatte vorhandenen Standard-Betriebssystem (z.B. Windows Vista), sondern mit dem auf der CD-ROM befindlichen Betriebssystem (z.B. LINUX). Die CD-ROM auf der sich die G DATA Software befindet, enthält nicht nur die G DATA Antiviren-Software zur Installation unter Windows, sondern funktioniert gleichzeitig als BootCD.

■ **Wie kann mein Computer von CD-ROM booten?**

Damit der Computer von CD-ROM booten kann, muss das BIOS (also das Basisprogramm, das dafür zuständig ist, dass z.B. Windows beim Start des Computers gestartet wird) entsprechend eingestellt sein. Sollte dies nicht der Fall sein, stellen Sie die Bootreihenfolge vorher im BIOS auf „**CD-ROM; C:**“ um. Auf diese Weise wird das CD-ROM-Laufwerk zum „**1st Boot Device**“ und die Festplattenpartition mit Ihrem Windows-Betriebssystem zum „**2nd Boot Device**“. Wenn nun die BootCD im CD-ROM-Laufwerk liegt, wird von dieser eine spezielle Linux-basierte G DATA Antiviren-Software gestartet. Sollte die BootCD nicht im CD-ROM-Laufwerk liegen, wird nach einigen Sekunden automatisch Ihr Windows-System gestartet. Üblicherweise gelangen Sie zum BIOS-Setup, indem Sie beim Hochfahren (= Booten) des Rechners die **ENTF**-Taste drücken. Wie Sie die

Einstellungen in Ihrem BIOS-Setup verändern, lesen Sie bitte in der Dokumentation Ihres Computers. Nach dem BootScan und der Installation der G DATA Antiviren-Software sollten Sie die Einstellung im BIOS möglichst bald auf „C“ zurückstellen, da diese Einstellung einen effektiven Schutz gegen Bootsekturviren darstellt, die sich z.B. auf versehentlich eingelegten Datenträgern befinden.

■ Installationsvorgang

Die Installation der Software ist ausgesprochen unkompliziert. Starten Sie einfach Ihr Windows und legen die Software-CD-ROM in Ihr CD-ROM-Laufwerk ein. Es öffnet sich automatisch ein Installationsfenster, welches Ihnen folgende Optionen bietet:

- **Installieren:** Hiermit starten Sie die Installation der Software auf Ihrem Computer. Sollten Sie die Software schon auf Ihrem System installiert haben und die CD-ROM einlegen, erscheint hier der **Aktualisieren**-Button und Sie können schnell und unkompliziert Ihre alte Software-Version updaten oder im Rahmen des benutzerdefinierten Setup umkonfigurieren.
- **Durchsuchen:** Über den Windows-Explorer können Sie hier die Verzeichnisse der Software-CD-ROM sichten.
- **Abbrechen:** Über diesen Eintrag können Sie die den Autostart-Bildschirm schließen, ohne eine Aktion durchzuführen.

Klicken Sie auf nun auf den **Installieren**-Button.

■ Sollten Sie die **Autostart-Funktion Ihres CD-ROM-Laufwerks** nicht aktiviert haben, kann die Software den Installationsvorgang nicht automatisch starten. Suchen Sie dann alternativ durch Anklicken des Arbeitsplatz-Symbols auf Ihrem Desktop in der obersten Verzeichnisebene Ihres CD-ROM-Laufwerks die Datei „**setup**“ bzw. „**setup.exe**“ und starten diese.

■ Willkommen

Zur Installation der G DATA Antiviren-Software auf Ihrem Computer klicken Sie bitte auf den **Weiter**-Button.

■ Wenn Sie die Installation aus irgendwelchen Gründen abbrechen möchten, klicken Sie bitte auf den **Abbrechen**-Button, der in jedem Installationsfenster vorhanden ist. Beim Abbruch der Installation werden sämtliche schon auf Ihrem Computer installierte Daten gelöscht und das System in den Zustand zurückversetzt, den es vor dem Beginn der Installation hatte.

■ Lizenzvereinbarung

Nun erscheint ein Bildschirm mit den Lizenzvereinbarungen zur Nutzung der Software. Bitte lesen Sie sich diese aufmerksam durch und klicken auf „**Ich bin mit den Bedingungen dieser Lizenzvereinbarung einverstanden**“ um sämtlichen Bestimmungen des Lizenzvertrags zuzustimmen.

■ *Um sich den Lizenzvertrag komplett durchzulesen, können Sie den Text durch Anklicken der kleinen Pfeilsymbole mit der Maus nach oben und unten verschieben. Über den **Drucken**-Button können Sie sich die Vertragsbedingungen auch ausdrucken. Wenn Sie „**Nein**“ wählen, wird das Installationsprogramm abgebrochen. Für die Installation der Software müssen Sie dieser Lizenzvereinbarung zustimmen.*

■ Setup-Typ

Nun haben Sie die Möglichkeit, den Installationsumfang der Software zu bestimmen. Wählen Sie einfach die gewünschte Installationsvariante (**vollständig** oder **benutzerdefiniert**) mit der Maus an und klicken Sie dann auf den **Weiter**-Button. Die Software wird dann mit allen Komponenten installiert. In der Regel ist es sinnvoll, die G DATA Antivirensoftware vollständig zu installieren. Bei der benutzerdefinierten Installation haben Sie die Möglichkeit spezielle Komponenten der Software nicht mitzuinstallieren. Dies ist z.B. dann sinnvoll, wenn Sie die Software nur für sehr spezielle Einsatzgebiete nutzen möchten.

■ Zielpfad wählen

Hier haben Sie die Option, den Speicherort („**Zielordner**“) für die Programmdateien und den Namen für die Programmgruppe zu ändern.

■ *Generell sollte der Zielpfad nicht geändert werden. Nur in Fällen, wo z.B. auf der Windows-Partition Ihrer Festplatte zu wenig Speicherplatz zur Verfügung steht, kann es sinnvoll sein, die Software auf einer anderen Partition oder Festplatte zu installieren.*

■ Features wählen

Während bei der vollständigen Installation alle Module installiert werden, haben Sie bei der benutzerdefinierten Auswahl die Möglichkeit, gezielt die Module auszuwählen, die Sie benötigen.

- **AntiVirus:** Virenschutz mit DoubleScan-Technologie
- **Programmdateien:** Diese Komponente ist obligatorisch, wenn Sie die G DATA Antiviren-Software installieren möchten.

- **Virenwächter:** Der Wächter scannt Dateien vor dem Öffnen automatisch auf Viren. Sie können die G DATA Antiviren-Software auch ohne den Wächter verwenden, allerdings erfolgt dann keine permanente Antivirenkontrolle. Die Installation des Wächters ist generell zu empfehlen.
- **Analyse mit rechter Maustaste:** Die Analyse mit rechter Maustaste (per Kontextmenü) erlaubt es Ihnen, die G DATA Antiviren-Software aus dem Windows-Explorer heraus für eine bestimmte Datei oder einen bestimmten Ordner direkt mit einem Mausklick zu starten.
- **E-Mail-Virenblocker (Outlook):** Einbindung für Microsoft Outlook und Exchange. Prüft ein- und ausgehende Mails automatisch auf Viren und scannt komplette Post-Ordner. Wenn Sie Outlook nicht verwenden, braucht diese Option nicht installiert werden.
- **Boot-CD:** Ermöglicht die Erstellung einer aktualisierten CD-ROM zum BootScan. Da Sie mit der Boot-CD auch ein schon infiziertes Betriebssystem noch vor dem Start reparieren können, ist die Möglichkeit zur Boot-CD-Erstellung eine hilfreiche Komponente.
- **AntiSpam:** Mit AntiSpam können Sie unerwünschte Werbemails aus Ihrem POP3/IMAP-Mailprogramm ausfiltern.
- **Spamprüfung für Microsoft Outlook:** Wenn Sie als Mailprogramm Microsoft Outlook verwenden, sollten Sie dieses Feature installieren. Wenn Sie Microsoft Outlook oder ein anderes POP3-Programm UND Microsoft Outlook verwenden, sollten Sie die Spamprüfung sowohl für POP3/IMAP-Mailprogramme, als auch Microsoft Outlook aktivieren.
- **Firewall:** Legen Sie hier fest, ob eine Firewall zum Schutz vor Angriffen aus dem Internet installiert werden soll oder nicht.
- **Kindersicherung:** Mit der Kindersicherung können Sie ihre Kinder vor nicht kindgerechten Inhalten aus dem Internet schützen.
- **Webfilter:** Mit diesem Plugin für den Internet Explorer erhalten Sie einen wirksamen Schutz vor unerwünschten Popups, Phishing etc.
- **G DATA Shredder:** Der Datenschredder vernichtet nicht länger benötigte Dateien auf Wunsch vollständig und unwiederbringlich. Die Dateien können dann auch mit Datenrettungstools nicht wiederhergestellt werden.
- **Tuner:** Mit dem Tuner optimieren Sie Ihr System, entfernen unnötige Dateien aus der Registry, erhalten Hilfestellungen zur Defragmentierung und vieles mehr.
- **Backup:** Das Backup-Tool sichert Ihre wichtigen persönlichen Daten automatisch auf jedem beliebigen Medium.
- **TopSecret:** Diese Software verschlüsselt Ihre sensiblen Daten gegen unbefugten Zugriff.

 **Achtung:** Das Programm-Modul „TopSecret“ steht Ihnen nur auf 32-Bit-Systemen zur Verfügung. Auf 64-Bit-Systemen ist eine Installation nicht möglich.

■ Automatische Aktionen

Sie können schon während der Installation festlegen, ob die G DATA Antiviren-Software automatische Aktionen, wie das Update der Virensignaturen („**Virenupdate stündlich laden**“) und die Prüfung des Rechners in den empfohlenen Zeitabständen („**Rechner wöchentlich auf Viren prüfen**“) durchführen soll. Wenn Sie hier individuelle Einstellungen vornehmen wollen oder keine automatischen Aktionen wünschen, entfernen Sie einfach das Häkchen an der entsprechenden Auswahl. Wenn Sie das Feature „Backup“ installiert haben, können Sie auch während der Installation schon festlegen, dass eine Sicherheitskopie Ihrer persönlichen Daten wöchentlich erstellt wird.

■ Installationsabschluss

Nach Eingabe dieser Informationen startet die Installation der Software auf Ihrem System. Dieser Vorgang kann einige Minuten dauern und Ihnen wird über Fortschrittsbalken angezeigt, an welcher Position der Installation Sie sich gerade befinden. Nach erfolgreicher Installation erscheint ein Abschlussbildschirm. Klicken Sie einfach auf den „**Fertig stellen**“-Button. Sie können die Software (ggf. nach einem Neustart) jetzt direkt, über den Eintrag „**G DATA NotebookSecurity**“ unter „**Start > (Alle) Programme > G DATA NotebookSecurity**“ oder durch Anklicken des entsprechenden Symbols auf Ihrem Desktop starten.

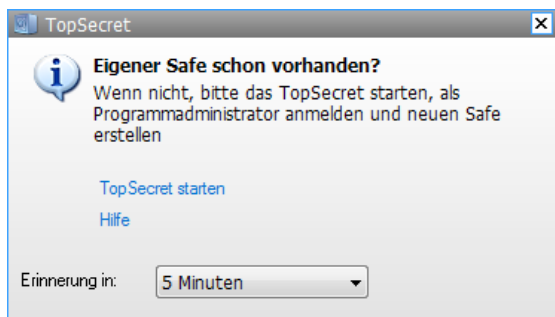
☐ *Je nach Installationsvariante kann es nach einem Rechner-Neustart noch einige Minuten dauern, bis Ihnen die Software zur Verfügung steht.*

Wenn Sie die Standardinstallation ausgewählt haben oder bei der benutzerdefinierten Installationsvariante den Wächter mitinstalliert haben, dann sehen Sie unten rechts in der Taskleiste das **Wächtersymbol**. Seine Funktion wird in dem Kapitel „**Security-Symbol**“ erläutert.



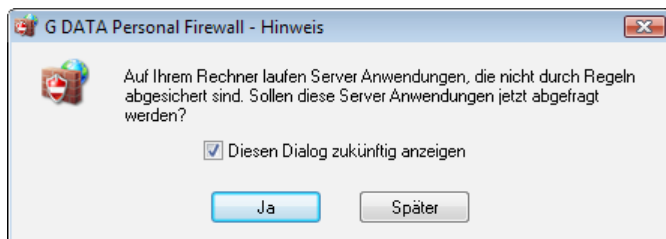
■ TopSecret-Administrator festlegen

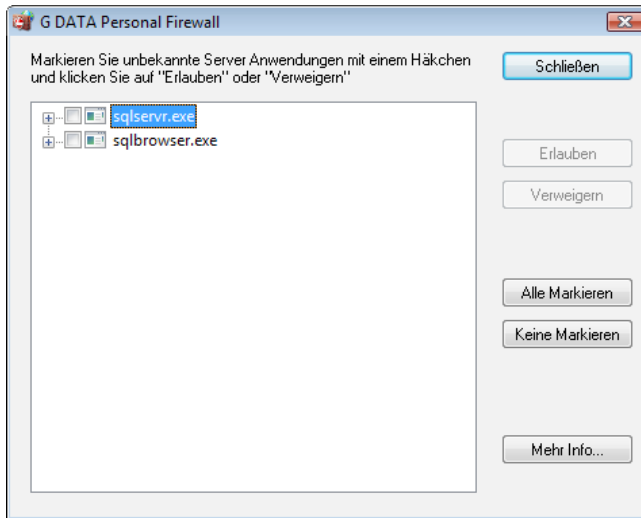
Die **G DATA TopSecret-Software** fragt nach der Installation in einem Infoscreen nach, ob Sie einen persönlichen Datensafe erstellen möchten. Dazu können Sie die G DATA TopSecret-Programmoberfläche über „**TopSecret starten**“ direkt aufrufen. Die Erinnerungsfunktion können Sie danach entfernen, wenn Sie unter „Erinnerung in:“ die Option „nicht weiter erinnern“ auswählen.



■ Firewall-Assistent

Sollten auf Ihrem Computer Server-Anwendungen laufen, die nicht durch vordefinierte Firewall-Regeln abgesichert sind, können Sie diese, sofort in den Firewall-Schutz der **G DATA Firewall** integrieren.

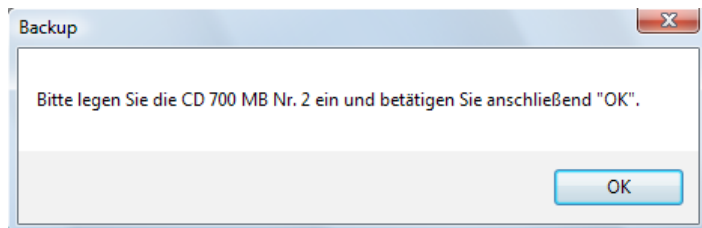
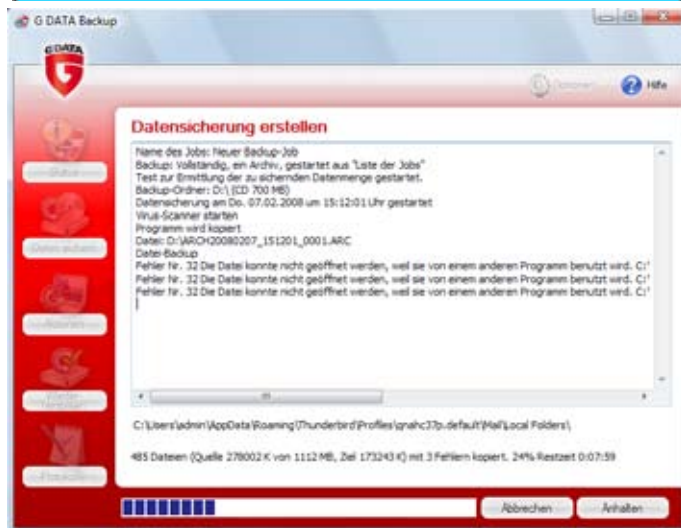
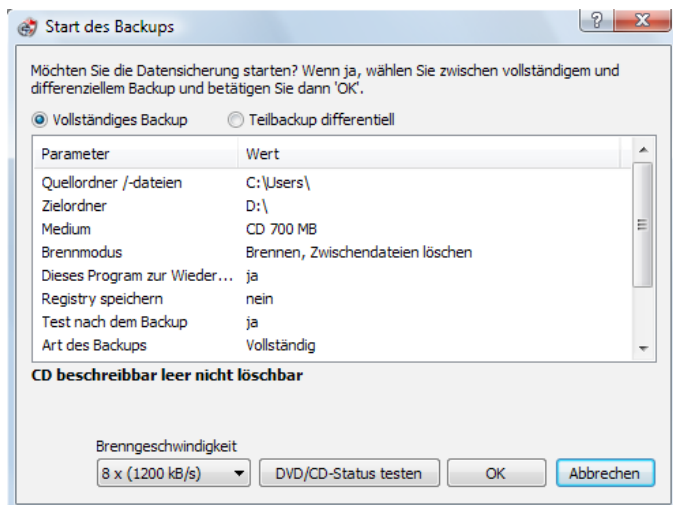




■ Start des Backups

Wenn Sie bei der Installation unter „**Automatische Aktionen**“ die wöchentliche Erstellung von Backups ausgewählt haben, öffnet sich die Backup-Software eine Stunde nach der Installation automatisch. Legen Sie dazu eine (wieder-)beschreibbare CD oder DVD in Ihr CD-/DVD-Laufwerk, klicken Sie auf den Button „**DVD/CD-Status testen**“ und klicken Sie dann einfach auf „**OK**“. Nun wird automatisch ein Backup Ihrer Daten auf CD oder DVD erstellt.

- *Sollte die Menge der Daten nicht auf eine CD oder DVD passen, werden Sie im Laufe des Backup-Vorgangs dazu aufgefordert, eine weitere (wieder-)beschreibbare CD/DVD einzulegen. Dieser Vorgang wird so lange wiederholt, bis all Ihre Daten gesichert sind!*
- *Natürlich können Sie mit der Backup-Software Ihre Daten auch auf anderen Festplatten, USB-Sticks oder sogar per FTP im Internet sichern. Wie Sie diese Funktionen nutzen, wird Ihnen ausführlich im Bereich „Backup“ erläutert.*
- *Wenn Sie Ihre Daten doch nicht sofort auf CD oder DVD sichern möchten, können Sie den Vorgang natürlich möglichst vor dem Einlegen eines (wieder-)beschreibbaren Datenträgers auch abbrechen und dann im Programmbereich „Backup“ nachträglich durchführen und die Optionen individuell an Ihre Bedürfnisse anpassen.*
- *Nachdem das Backup durchgeführt wurde, wird Ihnen der Inhalt der beschriebenen CD/DVD angezeigt. Hierbei handelt es sich um **ARC-Dateien**, also Archive, die Sie im Falle eines Datenverlustes über die Backup-Funktion der G DATA-Software wieder einspielen können.*



■ Tipps zur Deinstallation

Wenn Sie die G DATA Antivirensoftware irgendwann wieder deinstallieren möchten, können Sie dies am einfachsten durchführen, indem Sie im G DATA-Programmgruppeneintrag auf das „**Deinstallation**“-Icon klicken. Die Deinstallation erfolgt auf diese Weise vollautomatisch. Alternativ können Sie auch über die Windows-Systemsteuerung eine Deinstallation durchführen.

- **Windows XP und älter:** Klicken Sie in der Windows-Taskleiste auf „**Start**“ und wählen Sie den Ordner „**Einstellungen > Systemsteuerung > Software**“. Dort finden Sie auf der Karteikarte „**Installieren/Deinstallieren**“ die Möglichkeit, die G DATA-Software mit der Maus zu markieren. Klicken Sie dann auf den „**Hinzufügen/Entfernen**“-Button, um die Deinstallation durchzuführen.
- **Für Windows Vista:** Klicken Sie in der Windows-Taskleiste auf „**Start**“ und wählen Sie den Ordner „**Systemsteuerung**“ aus. Dort finden Sie den Punkt „**Programme > Programm deinstallieren**“. Wählen Sie hier die G DATA-Software aus der Liste aus und klicken dann auf den „**Deinstallieren**“-Button, um die Deinstallation durchzuführen.

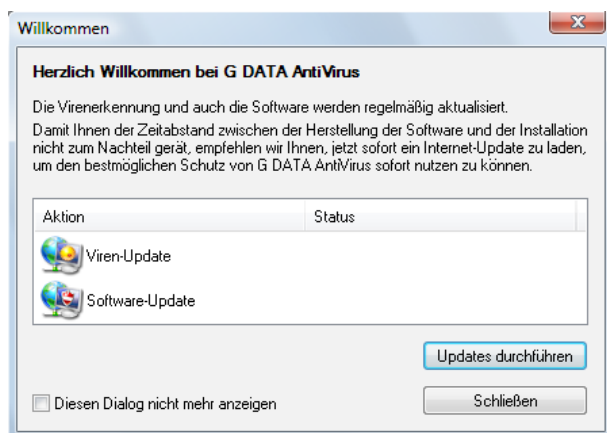
Sollten Sie während der Deinstallation noch Dateien im **Quarantäne**-Bereich der G DATA Antiviren-Software liegen haben, erfolgt eine Abfrage, ob diese Dateien gelöscht werden sollen oder nicht. Wenn Sie die Dateien nicht löschen, befinden diese sich weiterhin in einem speziellen G DATA-Ordner verschlüsselt auf Ihrem Computer und können auf diese Weise keinen Schaden anrichten. Diese Dateien stehen Ihnen erst wieder zur Bearbeitung zur Verfügung, wenn Sie die G DATA Antivirensoftware erneut auf Ihrem Computer installieren. Während der Deinstallation werden Sie gefragt, ob Sie „**Programmeinstellungen und Protokolle**“ löschen möchten. Wenn Sie diese Dateien nicht löschen, stehen Ihnen die Protokolle und Einstellungen bei einer erneuten Installation der Software wieder zur Verfügung. Schließen Sie die Deinstallation mit Anklicken des **Beenden**-Buttons ab. Die Software ist nun vollständig von Ihrem System deinstalliert.

Beim ersten Start

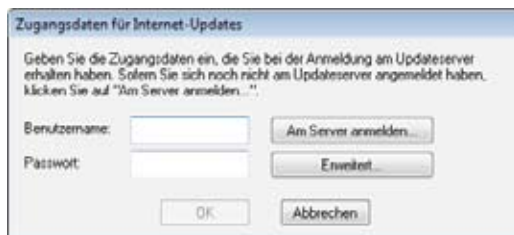
Beim ersten Start der G DATA-Software werden einige Parameter und Einstellungsoptionen abgefragt. Die Anzahl dieser Abfragen ist abhängig davon, welche Programm-Module Sie installiert haben und welche weiteren Einstellungen Sie bei der Installation vorgenommen haben.

■ Internet Update

Wenn Sie das die Software nach der Installation zum ersten Mal starten, öffnet sich ein Assistent, über den Sie sofort ein Internet-Update der Virensignaturen sowie ein Update eventueller Software-Aktualisierungen durchführen können.



Damit Ihnen der Zeitabstand zwischen der Herstellung der Software und der Installation nicht zum Nachteil gerät, empfehlen wir Ihnen, sofort dieses Update durchzuführen. Klicken Sie dazu einfach auf den Button „**Updates durchführen**“. Nun erscheint ein Fenster, in dem die Zugangsdaten für Internet-Updates abgefragt werden. Um diese Zugangsdaten zu erhalten, klicken Sie hier einfach auf den Button „**Am Server anmelden**“.



Es erscheint ein Eingabefenster, in dem Sie ihre **Registriernummer** und **Kundendaten** eingeben.

- Sollte die G DATA Antiviren-Software keine Verbindung mit dem Internet aufnehmen können, klicken Sie bitte auf den **Erweitert**-Button und nehmen die notwendigen Internet-Einstellungen vor.
- Die **Registriernummer** finden Sie auf der Rückseite des gedruckten Bedienungshandbuches. Wenn Sie die Software online gekauft haben, erhalten Sie die Registrierungsnummer in einer gesonderten E-Mail.

Klicken Sie nun auf den **Anmelden**-Button und Ihre Zugangsdaten werden auf dem G DATA-Updateserver generiert. Wenn die Anmeldung erfolgreich verlief, erscheint ein Info-Bildschirm mit dem Vermerk „**Die Anmeldung wurde erfolgreich durchgeführt**“, den Sie mit dem **Schließen**-Button verlassen können.

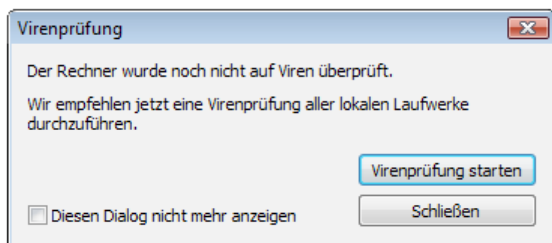
- Für Ihre Unterlagen und für etwaige Neuinstallationen der Software erhalten Sie Ihre Zugangsdaten auch per Mail zugesandt. Bitte vergewissern Sie sich deshalb, dass Ihre in der Online-Registrierung angegebene E-Mail-Adresse korrekt ist; ansonsten stehen Ihnen die Zugangsdaten nicht zur Verfügung.

Abschließend werden die Zugangsdaten automatisch in die ursprüngliche Eingabemaske übernommen und Sie können durch Anklicken des **OK**-Buttons den eigentlichen Update-Vorgang starten.

■ Sie können das Update auch jederzeit nachträglich durchführen.

■ Virenprüfung

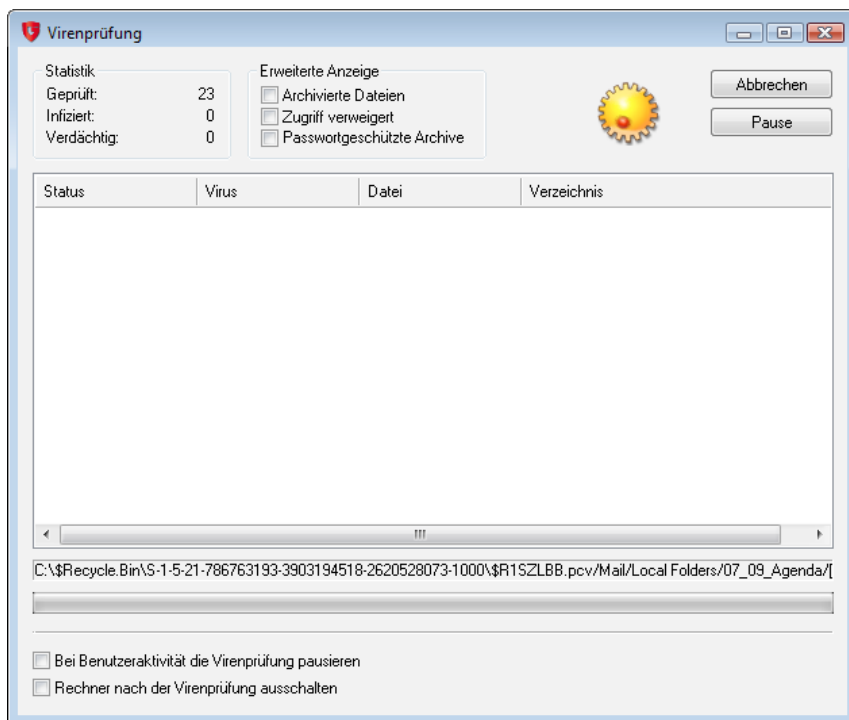
Gerade wenn Ihr Computer vor der Nutzung der G DATA Antivirensoftware noch nicht durch ein Virenprogramm geschützt war, ist es ratsam, nach der Installation und dem Internet Update der Virensignaturen sofort eine Überprüfung des Rechners auf Virenbefall vorzunehmen. Mit dem Assistenten, der beim ersten Start der Software erscheint, können Sie diese Prüfung direkt vornehmen.



Wenn Sie den Button „**Virenprüfung starten**“ drücken, startet die Überprüfung Ihres Rechners auf Virenbefall mit den Standardeinstellungen. Dazu öffnet sich ein Fenster, in dem Sie über den Verlauf der Virenüberprüfung informiert werden. Bitte beachten Sie, dass eine Virenprüfung je nach Rechnergeschwindigkeit und der Menge der auf der Festplatte vorhandenen Daten eine Stunde oder länger dauern kann. Nach Abschluss der Virenprüfung erscheint ein **Schließen**-Button, über den Sie den Virenprüfungsbildschirm beenden können.

■ Generell können Sie Ihren Computer während der Virenüberprüfung ganz normal weiterverwenden, sollte es bei speicherintensiven Anwendungen doch zu Verzögerungen kommen, können Sie die Virenprüfung über den **Pause**-Button auch anhalten und zu einem späteren Zeitpunkt mit Anklicken von „**Fortsetzen**“ weiterführen.

■ Über den **Abbrechen**-Button stoppen Sie die Virenprüfung. Achtung! Ihr Rechner wurde in diesem Fall nicht vollständig auf Virenbefall untersucht. Sie sollten eine Virenkontrolle dann sobald wie möglich wiederholen.



Bei einem Virenfund erscheint ein Info-Fenster, in dem Ihnen das Programm verschiedene Optionen zur Verfügung stellt, wie mit dem Virus zu verfahren ist. Über den **Vireninformation**-Button können Sie sich online detaillierte Zusatzinfos zum gefundenen Virus anzeigen lassen.

In dem Info-Fenster können Sie festlegen, was bei Entdeckung einer infizierten Datei geschehen soll. Je nach dem, für welche Zwecke Sie Ihren Computer verwenden, sind hier unterschiedliche Einstellungen sinnvoll. So ist für Anwender, die viele Daten auf Ihrem Computer verwahren, die Option „**Desinfizieren (wenn nicht möglich: in Quarantäne verschieben)**“ eine empfehlenswerte Möglichkeit, da hier die Verbreitung des Virus unterbunden wird und trotzdem keine Datei auf dem Rechner gelöscht wird. Das direkte Löschen infizierter Dateien („**Infizierte Datei löschen**“) wird dagegen nur für die wenigsten Anwender sinnvoll sein. Die Nutzung des Quarantäne-Ordners über die Funktion „**Datei in Quarantäne verschieben**“ bieten den Vorteil, dass die Dateien im Quarantäne-Ordner sicher verwahrt sind, ohne weiteren Schaden anrichten zu können und Sie sich später Gedanken darüber machen können, wie Sie mit den Dateien verfahren möchten. Bei der Einstellung „**Nur protokollieren**“ wird im Dateisystem keine Änderung vorgenommen, sondern nur in einer Log-Datei festgehalten, dass sich eine möglicherweise infizierte Datei auf Ihrem System befindet.

Virenfund

Datei: Uninst.exe

Verzeichnis: C:\Program Files\DAEMON Tools SearchBar

Virus: not-a-virus:AdWare.Win32.SaveNow.az
(Engine A)

Vireninformation

Aktion

- ☐ Nur protokollieren
- ☒ Desinfizieren (wenn nicht möglich: in Quarantäne verschieben)
- ☐ Datei in die Quarantäne verschieben
- ☐ Infizierte Datei löschen

☐ Auf alle anwenden

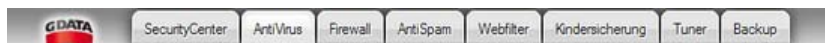
OK

Abbrechen

Allgemeine Programminformationen

■ Bedienung der Software

Die Bedienungsoberfläche der Software ist prinzipiell selbsterläuternd und übersichtlich gestaltet. Anhand unterschiedlicher Karteikarten wechseln Sie in das jeweilige Programm-Modul und können dort Aktionen durchführen, Voreinstellungen vornehmen oder Protokolle und Ergebnislisten überprüfen.

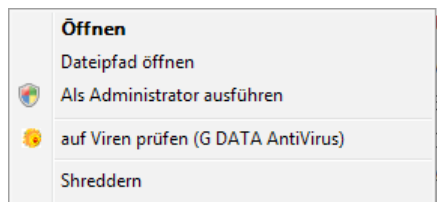


Um zwischen den einzelnen Programm-Modulen zu wechseln, klicken Sie einfach auf das jeweils oben angezeigte Register. Die Funktionselemente der jeweiligen Programm-Module werden Ihnen in den gleichnamigen Kapiteln erläutert.

- *Jedes dieser Module beinhaltet eine eigene Online-Hilfe, den Sie über den Hilfe-Button in der Menüleiste aufrufen können.*
- *Sollte einer der Programm-Module fehlen, kann es daran liegen, dass Sie das jeweilige Feature (z.B. die Firewall oder die Kindersicherung) bei der benutzerdefinierten Installation nicht mitinstalliert haben. Eine andere Möglichkeit ist die, dass Sie eine Programmversion besitzen, die das entsprechende Feature nicht beinhaltet.*

■ Windows Kontextmenü

Bei der Installation der Software wird eine Analysefunktion in das Windows-Kontextmenü eingefügt. Hiermit können Sie direkt Virenanalysen bestimmter verdächtiger Objekte durchführen: Dazu bewegen Sie die Maus auf das zu analysierende Objekt (Laufwerk, Verzeichnis, Datei) und betätigen die rechte Maustaste. Das Windows Kontextmenü öffnet sich. Durch Anwählen des Menüpunktes **„auf Viren prüfen (G DATA AntiVirus)“** wird automatisch eine Analyse des Objektes mit den Standardeinstellungen des Programmbereiches **„G DATA AntiVirus“** durchgeführt.



■ Shredder



Der **Shredder** steht Ihnen als Symbol auf dem Desktop zur Verfügung. Ziehen Sie einfach die Dateien, die Sie löschen möchten, auf das Shredder-Symbol. Eine Sicherheitsabfrage weist Sie darauf hin, dass Dateien im Shredder unwiederbringlich zerstört werden. Klicken Sie auf „**Ja**“, wenn Sie die Dateien tatsächlich auf diese Weise löschen möchten.

☐ *Sie können Ordner und Dateien auch über das Windows Kontextmenü mit dem Shredder löschen. Markieren Sie dazu einfach die gewünschten Dateien oder Ordner, klicken dann die rechte Maustaste und wählen den Eintrag „Shreddern“.*

■ Security-Symbol

Über das Security-Symbol, das sich in der Regel rechts unten in der **Taskleiste** Ihres Windows Desktops neben der Systemuhr befindet, können Sie immer feststellen, ob der Virenwächter aktiv ist.

- Der aktivierte Wächter zeigt ein rotweißes Schild.
- Falls der Wächter nicht aktiviert wurde, ist das Schild mit einem Achtung-Symbol markiert. Ein permanenter Virenschutz für Ihr System ist dann nicht gegeben.



Wenn Sie das Symbol mit der rechten Maustaste anklicken, erscheint ein Kontextmenü, mit dem Sie grundlegende Sicherheitsaspekte der Software steuern können.



Folgende Funktionen stehen Ihnen hier zur Verfügung:

- **Starten:** Hiermit rufen Sie die Programmoberfläche auf und können dort z.B. die Einstellungen für den Virenwächter vornehmen.
- **Wächter einschalten / ausschalten:** Hiermit können Sie den Wächter bei Bedarf abschalten. Dies kann z.B. dann sinnvoll sein, wenn Sie auf Ihrer Festplatte große Dateimengen von einem Ort zum anderen kopieren oder speicherplatzintensive Rechengvorgängen (z.B. DVDs kopieren o.ä.) ablaufen lassen. Sie sollten den Wächter nur so lange abschalten, wie es unbedingt nötig ist und darauf achten, dass das System während dieses Zeitraums möglichst nicht mit dem Internet verbunden ist oder auf neue ungeprüfte Daten (z.B. über CDs, DVDs, Speicherkarten oder USB-Sticks) zugreifen kann. Sie können den Wächter über diese Funktion nur für bestimmte Zeitintervalle (maximal bis zum nächsten Neustart) ausschalten. Wenn Sie den Wächter komplett ausschalten wollen, können Sie das über die G DATA-Programmoberfläche durchführen.
- **Firewall-Notaus aktivieren / aufheben:** Wenn Sie den Eindruck haben, dass ganz aktuell ein Angriff auf Ihren Computer erfolgt oder Sie z.B. das Gefühl haben, dass sich gerade ein Dialer gegen Ihren Willen verbinden will, können Sie mit dem **Notaus**-Button den Zugriff Ihres Computers auf das Netzwerk vollständig blockieren. Dieser Modus entspricht der physikalischen Trennung des Computers vom Internet und/oder vom lokalen Netzwerk.
- **Firewall ausschalten:** Sie können die Firewall bei Bedarf auch abschalten. Ihr Computer ist dann weiterhin mit dem Internet und anderen Netzwerken verbunden, wird von der Firewall aber nicht mehr vor Angriffen oder Spionage-Attacken geschützt. Sie können die Firewall über diese Funktion nur für bestimmte Zeitintervalle (maximal bis zum nächsten Neustart) ausschalten. Wenn Sie die Firewall komplett ausschalten wollen, können Sie das über die G DATA-Programmoberfläche erledigen.
- **Viren-Update:** Auch unabhängig von zeitplangesteuerten Virensignatur-Updates können Sie über die Funktion „**Viren-Update**“ ihre Virensignaturen jederzeit auf den neuesten Stand bringen.
- **Statistik:** Hier können Sie sich eine Statistik über die Prüfungsvorgänge des Virenwächters anzeigen lassen.

SecurityLock

Mit dem G DATA SecurityLock erhalten Sie ein Notebook-Schloss, dass den Diebstahl Ihres Notebooks erschwert. Um Ihr Notebook zu schützen, gehen Sie folgendermaßen vor:

- Legen Sie die das Kabel um einen festen Gegenstand (z.B. Heizungsrohr, am Boden montiertes Tischbein o.ä.) und ziehen Sie das Zylinderschloss durch die Kabelschlinge.

- Stecken Sie nun das Zylinderschloss in den dafür vorgesehenen Notebook-Schlitz (6 mm lang, 3 mm breit, meist an der linken oder rechten hinteren Seite des Notebook-Gehäuses). Dieser Schlitz wird auch als Kensington-Schlitz bezeichnet und ist speziell für die Verwendung mit Notebook-Schlössern vorgesehen.
- Schließen Sie das Zylinderschloss mit einem der beiden beiliegenden Schlüssel ab.

■ *Mit professionellem Werkzeug oder genügend krimineller Energie stellt ein Notebook-Schloss für professionelle Diebe nur ein geringes Hindernis dar, allerdings sind die meisten Notebook-Diebstähle Gelegenheitsdelikte, bei denen ein unbeaufsichtigtes Notebook einfach mitgenommen wird. Gegen diese Art von Diebstahl leistet ein Notebook-Schloss sehr gute Dienste! Generell gilt: Sie sollte Ihr Notebook an öffentlichen Orten wie z.B. Messen, Zugabteilen, Seminarräumen oder Gaststätten nie unbeaufsichtigt lassen! Selbst am Arbeitsplatz ist Ihr Notebook nicht wirklich sicher. Verwenden Sie deshalb das Notebook-Schloss wie beschrieben und geben Sie am besten Dieben erst gar keine Gelegenheit, Ihren Computer zu stehlen.*

■ *Die naheliegende Idee, das Notebook an ein Tischbein anzuschließen, macht nur dann Sinn, wenn der Tisch entweder sehr schwer oder das Tischbein im Boden verankert ist. Ein gewöhnlicher Tisch, der z.B. in Seminarräumen steht, ist schnell angehoben und die Notebook-Schloss-Schlaufe nach unten hin weggezogen. Auf diese Weise ist ein Schutz Ihres Notebooks vor Gelegenheitsdieben also nur sehr bedingt gegeben.*

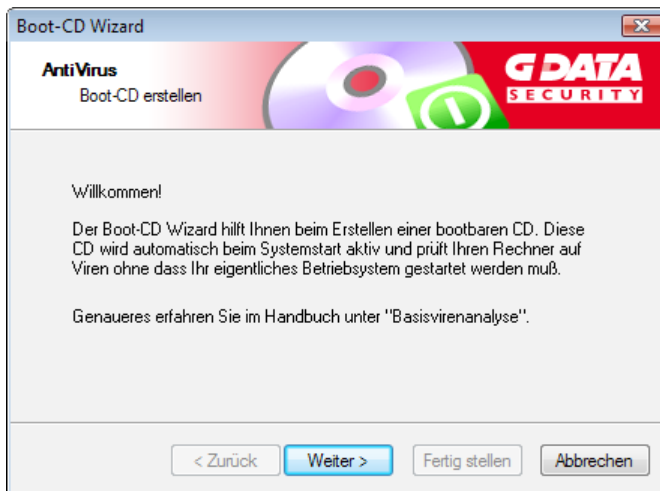


■ AntiVirus Boot-CD erstellen

In der Programmgruppe können Sie unter dem Eintrag **“AntiVirus Boot-CD erstellen”** eine LINUX-basierte Boot-CD für den BootScan erstellen. Im Gegensatz zum BootScan mit der Programm-DVD werden hier auch offline automatisch die jeweils aktuellsten Virensignaturen verwendet und die CD kann auch für Rechner mit CD-ROM-Laufwerken verwendet werden.

Die Boot-CD kann Ihnen auf anderen Rechnern, die noch nicht von G DATA geschützt sind, bei Virenbefall schnell und unkompliziert ein virenfreies System erzeugen, auf dem Sie dann eine Antivirensoftware zum permanenten Schutz installieren sollten.

Die Erzeugung der Boot-CD erfolgt mit Hilfe eines Assistenten, der Ihnen sämtliche Arbeitsschritte ausführlich erläutert.



■ BootScan

Der BootScan ist die wirksamste und sicherste Methode zur Erkennung und Beseitigung aktiver Rootkits. Sie sollten in regelmäßigen Abständen (z.B. wöchentlich) einen BootScan durchführen. Legen Sie hierzu diese CD wieder ein und starten Ihren Rechner anschließend neu.

- *Sie sollten niemals versuchen, ein Rootkit im geladenen Zustand unter Windows zu entfernen. Die Folge könnten erhebliche Systemschäden sein.*

SecurityCenter

Das **SecurityCenter** liefert Ihnen übersichtlich alle relevanten Informationen über den Status aller Programmkomponenten der G DATA Software. Neben Textinformationen wie z.B. „**aktiv**“ oder „**nicht aktiv**“ wird der Status der Komponenten auch grafisch dargestellt:

- ✓ Ein grünes **Häkchen** weist darauf hin, dass die jeweilige Komponente aktiv ist und ihre Schutzfunktion erfüllt.
- ⊘ Ein rotes **Verbotsschild** informiert darüber, dass die entsprechende Komponente nicht aktiv ist und die jeweilige Schutzfunktion nicht zur Verfügung steht.

Wenn Sie auf einen dieser Einträge klicken, gelangen Sie direkt zum jeweiligen Programmbereich, in dem Sie sicherheitsrelevante Einstellungen vornehmen können. Wenn Sie z.B. auf den Eintrag „**Datum der Virensignaturen**“ klicken, weil diese laut SecurityCenter veraltet sind, gelangen Sie automatisch in den Programmbereich „**AntiVirus**“ und können dort die Virensignaturen direkt online aktualisieren.



■ Bitte beachten Sie, dass das SecurityCenter einige Sekunden benötigt, um den neuen Status der G DATA Software zu ermitteln. In dieser Zeit stehen die Symbole auf „inaktiv“. Dies bedeutet allerdings nicht, dass Ihr System in diesem Moment nicht geschützt ist.

■ Bedienung der Software

Die Bedienung von AntiVirus ist prinzipiell selbsterläuternd und übersichtlich gestaltet. Anhand unterschiedlicher **Karteikarten**, die Sie über die links im AntiVirus angezeigten Symbole anwählen können, wechseln Sie in den jeweiligen Programmbereich und können dort Aktionen durchführen, Voreinstellungen vornehmen oder Protokolle und Ergebnislisten überprüfen.



Folgende **Programmbereiche** stehen Ihnen zur Verfügung und werden Ihnen in den gleichnamigen Kapiteln dieser Bedienungsanleitung ausführlich erläutert.

- **Status-Bereich**
- **Aktionen-Bereich**
- **Zeitplan-Bereich**
- **Quarantäne-Bereich**
- **Protokolle-Bereich**

■ Menüleiste

In der Menüleiste stehen Ihnen folgende Funktionen zur Auswahl:



Über das Optionen-Menü können Sie grundlegende Einstellungen und Vorgaben für die Arbeit mit AntiVirus vornehmen. Die jeweiligen Bereiche werden Ihnen ausführlich in dem Kapitel „**Optionen**“ erläutert.



Hiermit rufen Sie das große G DATA-Virenlexikon auf, das Ihnen einen interessanten Einblick in die weitverzweigte Welt der Viren und Schadprogramme bietet. Da das Virenlexikon ständig aktualisiert wird, finden Sie dieses als Online-Lexikon im Internet. Ein Anklicken des **Virenlexikon**-Buttons baut deshalb eine Internet-Verbindung auf. Sollte keine Internetverbindung zur Verfügung stehen, kann das Virenlexikon nicht angezeigt werden.



Hiermit rufen Sie die Online-Hilfe auf.

■ Programmbereiche

■ Status-Bereich

Im **Status-Bereich** von AntiVirus erhalten Sie grundlegende Informationen zum aktuellen Zustand Ihres Systems und der Software. Diese finden sich rechts vom jeweiligen Eintrag als Text-, Zahl- oder Datumsangabe.



Ein grünes **Häkchen** weist darauf hin, dass die jeweilige Komponente aktiv ist und ihre Schutzfunktion erfüllt.



Ein rotes **Verbotsschild** informiert darüber, dass die entsprechende Komponente nicht aktiv ist und die jeweilige Schutzfunktion nicht zur Verfügung steht.



Wenn sich die Programmoberfläche öffnet, sind für kurze Zeit die meisten Symbole im Achtung-Modus. Das heißt nicht, dass AntiVirus Ihren Computer in diesem Moment nicht schützt. Hier handelt es sich ganz im Gegenteil um eine interne Überprüfung des Virenschutz-Status, die Ihnen anzeigt, dass hier ein automatischer Check der Funktionen erfolgt.



Durch doppeltes Anklicken des jeweiligen Eintrags (oder durch Auswählen des Eintrags und Anklicken des **Bearbeiten**-Buttons) können Sie hier direkt Aktionen vornehmen oder in den jeweiligen Programmbereich wechseln. Sobald Sie die Einstellungen einer Komponente mit Achtung-Symbol optimiert haben, wechselt das Symbol im Status-Bereich wieder auf das grüne Häkchensymbol.

■ Virenwächter



Der Virenwächter überprüft automatisch Dateizugriffe auf Viren und sollte generell so eingestellt sein, dass er auf Ihrem Computer immer aktiv ist. Sie erkennen den aktivierten Wächter an dem Security-Symbol in der Taskleiste Ihres Computers.



Sollte der Wächter ausgeschaltet sein, weist Sie ein Achtung-Symbol darauf hin.

Der Wächter arbeitet auch dann, wenn Sie die AntiVirus-Programmoberfläche nicht geöffnet haben und kontrolliert Ihren Rechner im Hintergrund automatisch auf Viren ohne Sie dabei in Ihrer täglichen Arbeit zu beeinträchtigen. Wenn Sie den Eintrag „**Virenwächter**“ anklicken, öffnet sich ein **Wächtereinstellungen**-Menü, in dem Sie den Status des Virenwächters schnell zwischen „**eingeschaltet**“ und „**ausgeschaltet**“ umschalten können. Um die Wächterfunktionen genauer zu spezifizieren, klicken Sie bitte auf den **Erweitert**-Button. Auf diese Weise gelangen Sie in das Optionen-Menü des Wächters. Informationen zu den Einstellungsoptionen des Virenwächters erhalten Sie im Kapitel „**Optionen > Wächter**“.

■ E-Mail Virenblocker

Der E-Mail Virenblocker überprüft neue E-Mails auf Viren. Sie sollten den E-Mail Virenblocker immer aktiviert haben. Wenn Sie diesen Eintrag doppelt anklicken, öffnet sich eine Infobox, in der statistische Angaben zum E-Mail Virenblocker angezeigt werden. Über den **Aktualisieren**-Button können Sie diese Statistik auf den neuesten Stand bringen, wenn in der Zwischenzeit neue E-Mails eingetroffen sein sollten. Über den **Optionen**-Button gelangen Sie zum Konfigurationsmenü für den E-Mail Virenblocker. Hier können Sie z.B. die E-Mail-Überprüfung auf neu installierte E-Mail-Programme ausweiten und globale Einstellungen vornehmen. Informationen hierzu erhalten Sie in den Kapiteln „**Optionen > E-Mail-Schutz**“ und „**Optionen > E-Mail-Prüfung**“.

■ OutbreakShield

Mit dem OutbreakShield können Schädlinge in Massenmails schon erkannt und bekämpft werden, bevor aktualisierte Virensignaturen dafür verfügbar sind. Das OutbreakShield erfragt dabei über das Internet besondere Häufungen von verdächtigen Mails und schließt dabei quasi in Echtzeit die Lücke, die zwischen dem Beginn eines Massenmailings und seiner Bekämpfung durch speziell angepasste Virensignaturen besteht. Das OutbreakShield ist in den E-Mail Virenblocker integriert.

 *Um das OutbreakShield zu an- oder abzuschalten, setzen Sie einfach das OutbreakShield-Häkchen unter „Optionen > E-Mail-Prüfung“.*

■ Automatische Updates

Hier wird Ihnen angezeigt, ob die Internet-Updates der Virensignaturen vom G DATA AntiVirus-Server automatisch erfolgen oder nicht. Wenn Sie diesen Eintrag anklicken, gelangen Sie automatisch in den **Zeitplan**-Bereich der Software, in dem Sie die automatischen Updates definieren können. Lesen Sie hierzu bitte das Kapitel „**Programmbereiche > Zeitplan-Bereich**“ und seine Unterkapitel.

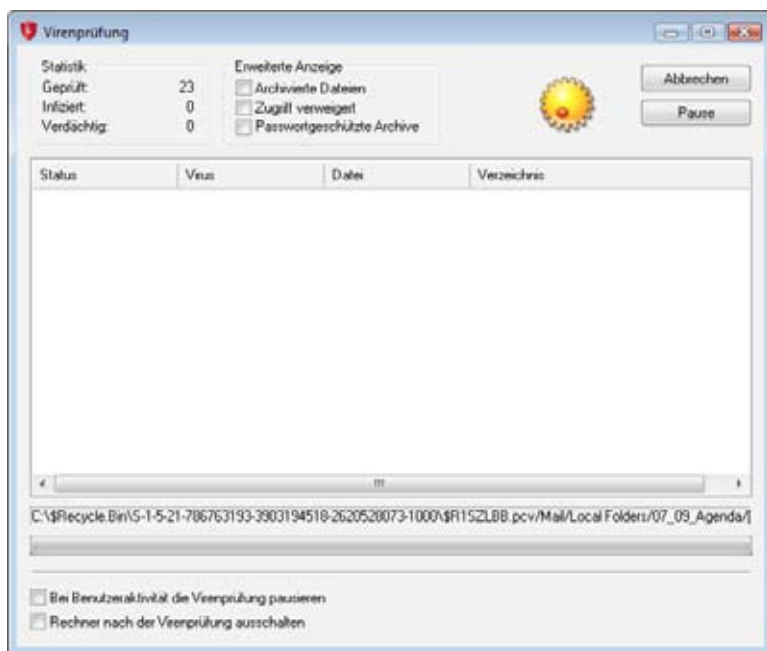
■ Datum der Virensignaturen

Je aktueller die Virensignaturen, desto sicherer ist Ihr Virenschutz. Sie sollten die Virensignaturen so oft wie möglich updaten. Wenn Sie diesen Eintrag doppelt anklicken, können Sie sofort eine Aktualisierung der Virensignaturen durchführen. Beantworten Sie die Frage „**Möchten Sie die Virensignaturen jetzt aktualisieren?**“ einfach durch Anklicken des **Ja**-Buttons. Nach einem Internet-Update stehen Ihnen die neuen Virensignaturen sofort zur Verfügung. Sie müssen die AntiVirus-Software nicht erneut starten, um mit den neuen Virendaten zu arbeiten. Sie haben auch

die Möglichkeit, das Internet-Update neuer Virensignaturen automatisch nach einem bestimmten Zeitplan durchführen zu lassen. Lesen Sie hierzu bitte das Kapitel „**Programmbereiche > Zeitplan-Bereich**“.

■ Letzte Analyse des Rechners

Regelmäßige Analysen erhöhen die Sicherheit vor Viren. Überprüfen Sie Ihren Rechner am besten nach jedem Internet-Update der Virensignaturen. Wenn Sie diesen Eintrag doppelt anklicken, können Sie sofort eine Analyse des Rechners auf Virenbefall durchführen. Beantworten Sie dazu einfach die Fragen „**Möchten Sie Ihren Rechner jetzt auf Viren überprüfen?**“ einfach durch Anklicken des **Ja**-Buttons. Während der Virenüberprüfung öffnet sich ein Fenster, in dem statistische Angaben und Informationen zur Virenanalyse angezeigt werden.



Unter „**Statistik**“ wird Ihnen angezeigt, wie viele Dateien überprüft wurden und wie viele davon gegebenenfalls infiziert sind oder verdächtig wirken. Im Anzeigefenster werden wichtige Informationen und Ergebnisse der Virenanalyse angezeigt. So werden hier auch infizierte Dateien aufgelistet. Virenfunde können Sie hier direkt bearbeiten und entscheiden, wie Sie damit verfahren möchten. Je nachdem, welche Häkchenfelder Sie unter „**Anzeige**“ aktiviert haben, erhalten Sie hier auch Informationen über archivierte Dateien, passwortgeschützte Archive und Dateien, auf die der Zugriff verweigert wurde.

- **Archivierte Dateien:** Hier können Sie festlegen, ob jeder einzelne Virenfund in einem Archiv angezeigt wird oder nur eine Zusammenfassung für das gesamte Archiv. So werde z.B. bei eingeschalteter Option bei einem Postfach mit 100 infizierten Dateien 101 Einträge angezeigt. Wenn die Option nicht eingeschaltet ist, wird lediglich mit einem Eintrag darauf hingewiesen, dass sich in dem Postfach-Archiv Viren befinden
- **Zugriff verweigert:** Generell gibt es unter Windows Dateien, die von Anwendungen exklusiv verwendet werden und deshalb von AntiVirus nicht überprüft werden können, solange diese Anwendungen laufen. Am besten sollten Sie deshalb während einer Virenprüfung möglichst keine anderen Programme auf Ihrem System laufen lassen. Wenn Sie hier ein Häkchen setzen, zeigt Ihnen AntiVirus die Dateien an, die nicht überprüft werden konnten.
- **Passwortgeschützte Archive:** Solange ein Archiv passwortgeschützt ist, kann AntiVirus die Dateien dieses Archives nicht auf Virenbefall überprüfen. Solange dieses Archiv nicht entpackt wird, stellt ein darin enthaltener Virus auch kein Sicherheitsrisiko für Ihr System dar. Wenn Sie Ihren AntiVirus-Wächter aktiviert haben, wird der Virus automatisch erkannt und bekämpft, sobald Sie das Archiv entpacken. Dazu muss im Wächter allerdings die Option „**Beim Schreiben prüfen**“ aktiviert sein. Lesen Sie hierzu bitte das Kapitel „**Optionen > Wächter**“. Wenn Sie das Häkchen bei „**Passwortgeschützte Archive**“ setzen, informiert AntiVirus Sie darüber, welche passwortgeschützten Archive es nicht überprüfen konnte.

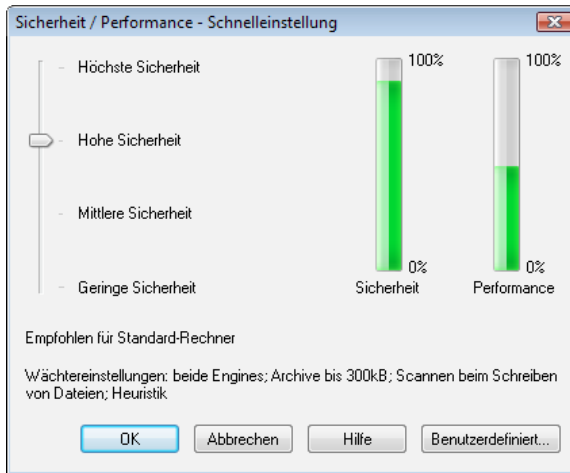
Ein Fortschrittsbalken im unteren Bereich des Fensters zeigt Ihnen, wie viel Prozent Ihres Systems schon überprüft wurden. In der Zeile darüber wird die aktuell geprüfte Datei mit kompletter Pfadangabe angezeigt. Über den **Abbrechen**-Button unterbrechen Sie die Analyse. Ihr System wurde in diesem Fall nicht vollständig auf Virenbefall untersucht. Wenn die Analyse vollständig durchgeführt wurde, erscheint ein **Schließen**-Button, über den Sie das Virenprüfung-Fenster wieder verlassen können. Das Ergebnis der Virenanalyse kann im Protokolle-Bereich eingesehen werden. Wie Sie die Virenanalyse individuell auf die Bedürfnisse Ihres Systems konfigurieren, lesen Sie in dem Kapitel „**Optionen > Virenprüfung**“.

■ Dateien in der Quarantäne

Im Quarantäne-Bereich werden verdächtige Dateien automatisch durch Verschlüsselung unschädlich gemacht und können von dort aus weiterbearbeitet werden. Wenn die infizierte Datei unbedingt benötigt wird, kann sie auch im infizierten Zustand wieder an ihren Ursprungsort zurückverschoben werden. Durch doppeltes Anklicken des Eintrags „**Dateien in der Quarantäne**“ gelangen Sie automatisch in den Quarantäne-Bereich. Lesen Sie hierzu das Kapitel „**Programmbereiche > Quarantäne-Bereich**“.

■ Sicherheit / Performance

Zwangsläufig sorgt eine permanente Überwachung Ihres Rechners für leichte Geschwindigkeitseinbußen. Sollten diese sich bei Ihnen tatsächlich störend bemerkbar machen, können Sie über die Funktion „**Sicherheit / Performance**“ zwischen dem Sicherheitsaspekt und der Performance Ihres Rechners abwägen und auf diese Weise den permanent aktiven **Virenwächter** auf Ihr System abstimmen.



Sie haben folgende Einstellungsmöglichkeiten:

- **Höchste Sicherheit** (nur empfohlen für sehr schnelle Rechner): beide Engines aktiv; Archive werden geprüft; Scannen beim Schreiben von Dateien; Heuristische Analyse aktiv.
- **Hohe Sicherheit** (empfohlen für Standard-Rechner): beide Engines aktiv; Archive bis 300 kB Größe werden geprüft; Scannen beim Schreiben von Dateien; Heuristische Analyse aktiv.
- **Mittlere Sicherheit** (nur empfohlen für langsame Rechner): nur Hauptengine aktiv; Archive werden nicht geprüft; Scannen beim Schreiben von Dateien; Heuristische Analyse aktiv.
- **Geringe Sicherheit** (nur empfohlen für sehr langsame Rechner): nur Hauptengine aktiv; Archive werden nicht geprüft; nur Programmdateien und Dokumente werden überprüft; Heuristische Analyse aktiv.

Wenn Sie mit den standardmäßig auszuwählenden Voreinstellungen für den Wächter nicht zufrieden sind, können Sie über den Button „**benutzerdefiniert**“ den Wächter auch individuell konfigurieren. Wie dies funktioniert und welche Bedeutung der hier aufgeführten Leistungsspezifika haben, wird ausführlich im Kapitel „**Optionen > Wächter**“ erläutert.

■ Aktionen-Bereich

Im Aktionen-Bereich können Sie Virenprüfungen direkt ausführen, unabhängig von zeitlichen Vorgaben für die automatischen Virenprüfungen, die Sie im Zeitplan-Bereich festlegen können. Bei der Virenprüfung haben Sie die Möglichkeit, die Prüfung auf bestimmte Bereiche bzw. Medien zu beschränken. So können Sie z.B. mit der Funktion **„Rechner prüfen“** Ihren kompletten PC kontrollieren, haben aber auch die Optionen, nur eingelegte Disketten oder CD-ROMs zu überprüfen. Über **„Verzeichnisse/Dateien prüfen“** können Sie auch festlegen, dass nur ausgewählte Bereiche Ihres Rechners kontrolliert werden (z.B. freigegebene Eingangsverzeichnisse einer Firewall oder nur die **„Eigene Dateien“**-Ordner). Außerdem können Sie von hier aus direkt ein Internet Update für Virensignaturen oder Software-Aktualisierungen von AntiVirus starten.



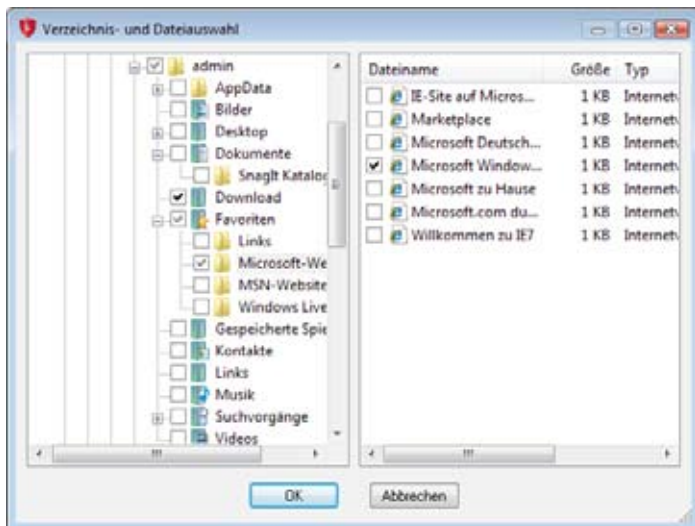
■ Die Virenprüfung der einzelnen Bereiche findet in dem Virenprüfungsfenster statt, wie es ausführlich im Kapitel „Programmbereiche > Status-Bereich > Letzte Analyse des Rechners“ beschrieben wird.

Folgende Optionen stehen Ihnen zur Verfügung:

- **Rechner prüfen:** Im Aktionen-Bereich haben Sie mit der Funktion **„Rechner prüfen“** die Möglichkeit, Ihren Rechner auf möglichen Virenbefall zu kontrollieren (also alle lokalen Festplatten und Systembereiche). Klicken Sie diese Funktion an und die Virenanalyse wird automatisch durchgeführt.

- **Diskette prüfen:** Prüfen Sie ins Diskettenlaufwerk eingelegte Disketten auf Virenbefall. Klicken Sie dazu einfach diese Aktion an.
- **CD-ROM prüfen:** Hier können Sie CD-ROMs oder DVD-ROMs in Ihrem CD-ROM- oder DVD-ROM-Laufwerk gezielt auf Virenbefall überprüfen. Klicken Sie einfach diese Aktion an und AntiVirus führt eine Virenanalyse durch.
- **Verzeichnisse/Dateien prüfen:** Hiermit prüfen Sie ausgewählte Laufwerke, Verzeichnisse oder Dateien auf Virenbefall. Wenn Sie diese Aktion doppelt anklicken (oder auf den **Start**-Button klicken), öffnet sich eine Verzeichnis- und Dateiauswahl. Hier können Sie gezielt einzelne Dateien und auch ganze Verzeichnisse auf Virenbefall überprüfen.
- **Speicher und Autostart:** Hierbei werden für alle laufenden Prozesse die Programmdateien und die dazugehörigen DLLs geprüft. Schadprogramme können so direkt aus dem Speicher entfernt werden (bzw. - wenn dies nicht durchführbar ist - beim nächsten Reboot entfernt werden). Aktive Viren können also direkt entfernt werden, ohne dass die ganze Festplatte durchsucht werden muss. Da diese Überprüfung relativ schnell durchgeführt werden kann, ist es empfehlenswert, sie z.B. im Rahmen einer automatischen Virenprüfung regelmäßig durchzuführen. Diese Funktion ist kein Ersatz für eine regelmäßige Virenkontrolle der gespeicherten Daten, sondern eine Ergänzung.
- **Dateien online prüfen:** Generell schützt Sie natürlich ihre G DATA-Antivirensoftware automatisch vor Infektionen, über die Online-Prüfung können Sie Dateien aber auch bei abgeschaltetem Virenschutz gezielt überprüfen. Wählen Sie dazu die verdächtige Datei aus und lassen Sie diese online auf Infektionen und schädliche Inhalte scannen. Sie können den Online-Dateiscanner auch einfach direkt aus Ihrem Internetbrowser heraus aufrufen: http://www.antiviruslab.com/scan_upload.php
- **Viren-Update:** Je aktueller die Virensignaturen, desto sicherer ist Ihr Virenschutz. Sie sollten die Virensignaturen so oft wie möglich updaten. Wenn Sie den Eintrag „**Viren-Update**“ im Aktionen-Bereich doppelklicken, können Sie sofort eine Aktualisierung der Virensignaturen durchführen. Nach einem Internet-Update stehen Ihnen die neuen Virensignaturen sofort zur Verfügung. Sie müssen AntiVirus nicht erneut starten, um mit den neuen Virendaten zu arbeiten.
- **Software-Update:** Über die Funktion „**Software-Update**“ laden Sie gegebenenfalls Software-Aktualisierungen von AntiVirus und seinen Komponenten vom G DATA-Server herunter. Wenn keine Software-Aktualisierungen auf dem Server vorliegen, werden Sie darüber durch eine Infobox informiert.

■ *Im Verzeichnisbaum (links) können Sie durch Anklicken der „+“-Symbole Verzeichnisse öffnen und auswählen, deren Inhalt dann in der Dateiansicht (rechts) angezeigt wird. Jedes Verzeichnis oder jede Datei, die Sie mit einem Häkchen versehen, wird von AntiVirus geprüft. Wenn in einem Verzeichnis nicht alle Dateien geprüft werden, findet sich an diesem Verzeichnis ein graues Häkchen.*



■ Zeitplan-Bereich

Im Zeitplan-Bereich können Sie Virenprüfungen und die Internet-Updates der Virensignaturen automatisieren, so dass diese zu bestimmten Zeiten selbständig von Ihrem Computer durchgeführt werden. Sie können verschiedene Schemata anlegen und diese auch parallel nebeneinander verwenden.

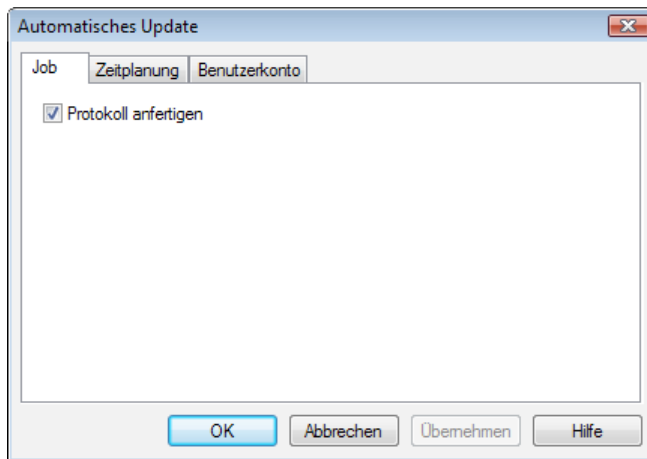


■ Automatische Updates

Über das Häkchenfeld vor dem Eintrag „**Virensignaturen**“ können Sie festlegen, ob ein automatisches Update der Virensignaturen erfolgen soll oder nicht. Wenn Sie das automatische Update nicht verwenden, sollten Sie darauf achten, regelmäßig selbst daran zu denken, die Virensignaturen von G DATA AntiVirus auf den neuesten Stand zu bringen. Um die Einstellungen des automatischen Updates zu ändern, klicken Sie bitte doppelt auf den Eintrag unter „**Automatische Updates**“ (oder markieren diesen und wählen den **Bearbeiten**-Button). Nun öffnet sich eine Box mit Karteikarten, in denen Sie die notwendigen Einstellungen vornehmen können. Um die vorgenommenen Änderungen zu übernehmen, klicken Sie bitte auf „**OK**“.

Job

Über das Häkchenfeld „**Protokoll anfertigen**“ können Sie festlegen, dass AntiVirus über den Update-Vorgang ein Protokoll anlegt. Dieses kann dann im Protokolle-Bereich (siehe Kapitel „**Programmbereiche > Protokolle-Bereich**“) eingesehen werden.



Zeitplanung

Über diese Karteikarte können Sie festlegen, wann und in welchem Rhythmus das automatische Update erfolgen soll. Unter „**Ausführen**“ geben Sie dazu eine Vorgabe vor, die Sie dann mit den Eingaben unter „**Zeitpunkt**“ und „**Wochentage**“ spezifizieren. Wenn Sie beim „**Internetverbindungsaufbau**“ auswählen, fallen die Vorgaben der Zeitplanung natürlich fort und AntiVirus führt das Update immer aus, wenn Ihr Rechner mit dem Internet verbunden wird.

■ Um unter „Zeitpunkt“ Daten- und Zeiteinträge zu ändern, markieren Sie einfach das Element, das Sie ändern möchten (z.B. Tag, Stunde, Monat, Jahr) mit der Maus und nutzen dann die Pfeiltasten oder die kleinen Pfeilsymbole rechts vom Eingabefeld, um sich im jeweiligen Element chronologisch zu bewegen.

Benutzerkonto

Hier kann ein Benutzerkonto auf dem Rechner angegeben werden, für das der Internet-Zugang konfiguriert ist.

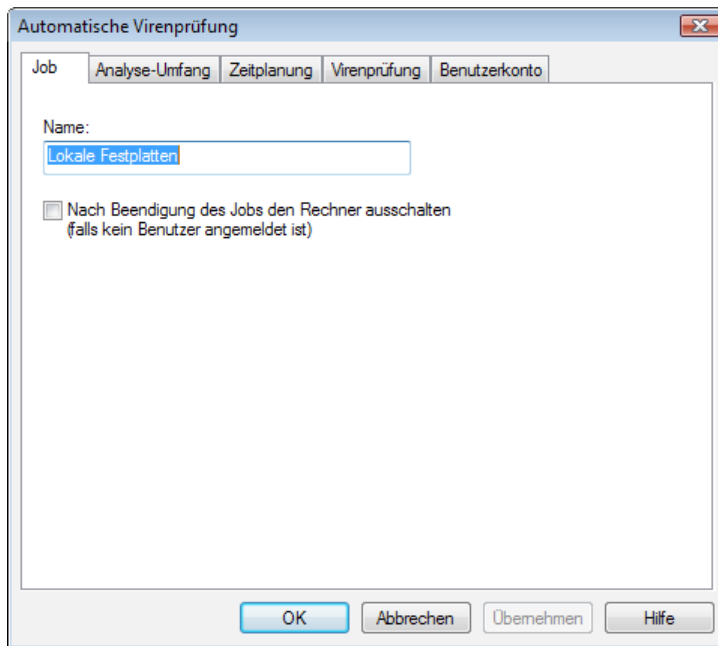
■ Es handelt sich hierbei nicht um den Benutzernamen und das Passwort für den Internet-Update-Support von AntiVirus, sondern um die Zugangsdaten für das Benutzerkonto, mit dem eine Internetverbindung möglich ist. Die notwendigen Angaben für das AntiVirus Internet-Update geben Sie unter „Optionen > Internet-Update“ ein, wie es im gleichnamigen Kapitel beschrieben wird.

■ Automatische Virenprüfungen

Über das Häkchenfeld unter dem Eintrag „**Lokale Festplatten**“ können Sie festlegen, ob eine automatische Update Virenprüfung erfolgen soll oder nicht. Wenn Sie die automatische Virenprüfung nicht verwenden, sollten Sie darauf achten, regelmäßig selbst daran zu denken, Ihr System regelmäßig auf Virenbefall zu überprüfen. Um die Einstellungen des automatischen Virenprüfungen zu ändern, klicken Sie bitte doppelt auf den Eintrag unter „**Automatische Virenprüfungen**“ (oder markieren diesen und wählen den **Bearbeiten**-Button). Nun öffnet sich eine Box mit Karteikarten, in denen Sie die notwendigen Einstellungen vornehmen können. Um die vorgenommenen Änderungen zu übernehmen, klicken Sie bitte auf „**OK**“. Sie können natürlich auch mehrere automatische Virenprüfungen zu verschiedenen Zeiten durchführen lassen. Um eine neue automatische Virenprüfung zu definieren, klicken Sie einfach auf den Button „**Neue Virenprüfung**“. So können Sie z.B. Bereiche, die zur täglichen Nutzung im Internet gedacht sind, auch täglich auf Viren überprüfen, während z.B. Ordner oder Festplatten, die der Archivierung dienen nur wöchentlich überprüft werden.

Job

Legen Sie hier fest, welchen Namen der neu eingerichtete Job haben soll. Zur Unterscheidung sind aussagekräftige Namen ratsam wie z.B. „**Lokale Festplatten (wöchentliche Überprüfung)**“ oder „**Archive (monatliche Überprüfung)**“.



Wenn Sie ein Häkchen bei „**Nach Beendigung des Jobs den Rechner ausschalten**“ setzen, wird der Rechner automatisch heruntergefahren, nachdem die automatische Analyse durchgeführt wurde.

- *Sollte zu diesem Zeitpunkt ein Benutzer angemeldet sein, wird der Rechner natürlich nicht heruntergefahren.*

Analyse-Umfang

Legen Sie hier fest, ob die Virenprüfung auf den Lokalen Festplattenlaufwerken stattfinden soll, ob Speicher und Autostartbereiche getestet werden sollen oder ob Sie nur bestimmte Verzeichnisse und Dateien prüfen wollen. Sollte dies der Fall sein, geben Sie bitte über den **Auswahl**-Button, die gewünschten Verzeichnisse an.

- *Im Verzeichnisbaum (links) können Sie durch Anklicken der „+“-Symbole Verzeichnisse öffnen und auswählen, deren Inhalt dann in der Dateiansicht (rechts) angezeigt wird. Jedes Verzeichnis oder jede Datei, die Sie mit einem Häkchen versehen, wird von AntiVirus geprüft. Wenn in einem Verzeichnis nicht alle Dateien geprüft werden, findet sich an diesem Verzeichnis ein graues Häkchen.*

Zeitplanung

Über diese Karteikarte können Sie festlegen, wann und in welchem Rhythmus die automatische Virenprüfung erfolgen soll. Unter „**Ausführen**“ geben Sie dazu eine Vorgabe vor, die Sie dann mit den Eingaben unter „**Zeitpunkt**“ und „**Wochentage**“ spezifizieren. Wenn Sie „**Beim Systemstart**“ auswählen, fallen die Vorgaben der Zeitplanung natürlich fort und AntiVirus führt die Prüfung immer aus, wenn Ihr Rechner neu gestartet wird.

■ Unter „*Täglich*“ können Sie mit Hilfe der Angaben unter „*Wochentage*“ z.B. bestimmen, dass Ihr Rechner nur an Werktagen die Virenprüfung durchführt oder eben nur an jedem zweiten Tag oder gezielt an Wochenenden, an denen er nicht zur Arbeit genutzt wird.

■ Um unter „*Zeitpunkt*“ Daten- und Zeiteinträge zu ändern, markieren Sie einfach das Element, das Sie ändern möchten (z.B. Tag, Stunde, Monat, Jahr) mit der Maus und nutzen dann die Pfeiltasten oder die kleinen Pfeilsymbole rechts vom Eingabefeld, um sich im jeweiligen Element chronologisch zu bewegen.

Virenprüfung

In diesem Bereich können Sie festlegen, mit welchen Einstellungen die automatische Virenprüfung stattfinden soll. Welche Bedeutung die hier einstellbaren Optionen haben, wird Ihnen ausführlich in dem Kapitel „**Optionen > Virenprüfung**“ erläutert.

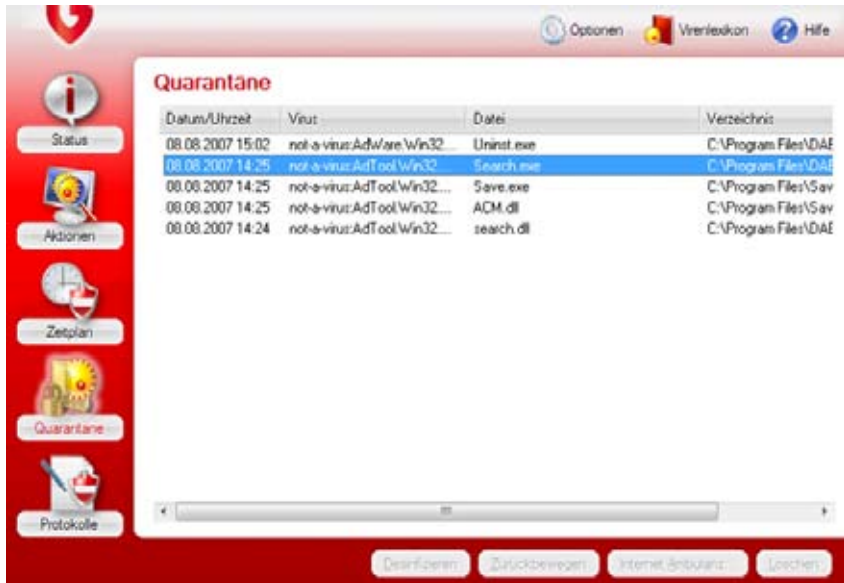
■ Die Einstellungsmöglichkeiten sind unter „*Optionen > Virenprüfung*“ und unter „*Programmbereiche > Zeitplan-Bereich > Automatische Virenprüfungen*“ identisch, allerdings können Sie beide unabhängig voneinander einstellen. So macht es z.B. Sinn, bei einer automatischen Virenprüfung (die am besten dann stattfinden sollte, wenn der Rechner nicht intensiv genutzt wird, z.B. am Wochenende) eine weit genauere Prüfung vorzunehmen, als bei einer direkten Virenprüfung, wie Sie Sie unter Aktionen (siehe Kapitel „*Programmbereiche > Aktionen-Bereich*“) durchführen lassen können.

Benutzerkonto

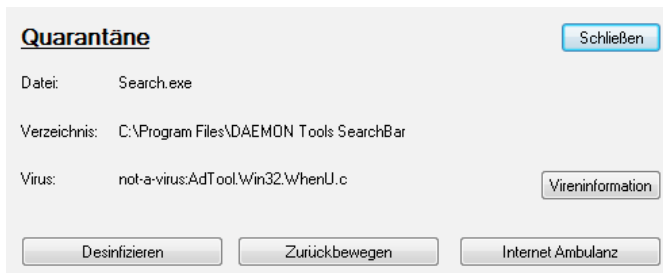
Hier kann das Benutzerkonto auf dem Rechner angegeben werden, auf dem die Virenprüfung stattfinden soll. Dieses Konto wird für den Zugriff auf Netzwerklaufwerke benötigt.

■ Quarantäne-Bereich

Während der Virenprüfung haben Sie die Möglichkeit, mit Virenfunden auf unterschiedliche Weise umzugehen. Eine Option ist es, die infizierte Datei in die Quarantäne zu verschieben. Die Quarantäne ist ein geschützter Bereich innerhalb von AntiVirus, in dem infizierte Dateien verschlüsselt gespeichert werden und auf diese Weise den Virus nicht mehr an andere Dateien weitergeben können. Die Dateien in der Quarantäne bleiben dabei in dem Zustand erhalten, in dem Sie AntiVirus vorgefunden hat und Sie können entscheiden, wie Sie weiterverfahen möchten.



■ Damit Viren automatisch in die Quarantäne verschoben werden, können Sie bei den Optionen für die Virenprüfung festlegen, was „Im Fall einer Infektion“ geschehen soll. Dies wird ausführlich im Kapitel „Optionen > Virenprüfung“ erläutert.



Sie haben dabei folgende Möglichkeiten:

■ Desinfizieren

In vielen Fällen können infizierte Dateien noch gerettet werden. AntiVirus entfernt dann die Virenbestandteile in der infizierten Datei und rekonstruiert auf diese Weise die nicht infizierte Originaldatei. Wenn eine Desinfektion erfolgreich ist, wird die Datei automatisch an den Ort zurückbewegt, an dem sie vor der Virenanalyse gespeichert war und steht Ihnen dort wieder uneingeschränkt zur Verfügung.

■ Zurückbewegen

Manchmal kann es nötig sein, eine infizierte Datei, die sich nicht desinfizieren lässt, aus der Quarantäne an ihren ursprünglichen Speicherort zurückzubewegen. Dies kann z.B. aus Gründen der Datenrettung erfolgen. Sie sollten diese Funktion nur im Ausnahmefall und unter strengen Sicherheitsmaßnahmen (z.B. Rechner vom Netzwerk/Internet trennen, vorheriges Backup uninfizierter Daten etc.) durchführen.

■ InternetAmbulanz

In bestimmten Fällen können Sie eine infizierte Datei, die Sie nicht desinfizieren können, über das Internet an die **Internet-Ambulanz** schicken:

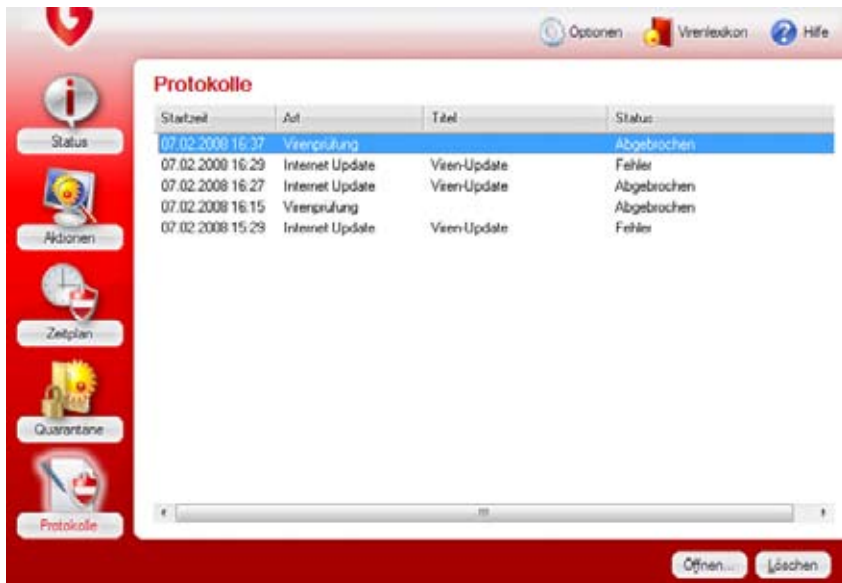
- **Für die Datei wurde ein Virenverdacht gemeldet. Bitte untersuchen Sie die Datei:** Wenn Sie die heuristische Analyse verwenden, kontrolliert AntiVirus verdächtige Dateien nicht nur anhand der aktuellen Virensignaturen, sondern schlägt auch automatisch Alarm, wenn eine Datei virenähnliche Elemente enthält. Hierbei handelt es sich in der Regel auch um Viren, in sehr seltenen Fällen aber auch um Fehlalarm. Wenn Sie eine solche Datei an die Internet-Ambulanz schicken, wird diese eingehend analysiert und untersucht. Sollte es sich um keinen Virus handeln, werden Sie entsprechend informiert.
- **Die Datei wurde als infiziert gemeldet. Ich glaube aber, dass Sie keinen Virus enthält. Bitte untersuchen Sie die Datei:** Sollten Sie ganz sicher davon ausgehen, dass es sich hierbei um keine Infektion handeln kann, schicken Sie die Datei bitte an die Internet-Ambulanz.
- **Ich benötige Informationen zu dem gefundenen Virus. Im Virenlexikon (www.antiviruslab.com) kann ich keine Informationen finden:** Selbstverständlich wird das Virenlexikon immer auf den neuesten Stand gebracht. Sollten Sie zum angegebenen Virus nichts im Virenlexikon gefunden haben, dann schicken Sie uns die infizierte Datei und das G DATA-Team kümmert sich um die Informationen.

■ Löschen

Wenn Sie die infizierte Datei nicht mehr benötigen, können Sie diese auch einfach aus der Quarantäne löschen.

■ Protokolle-Bereich

Im Protokolle-Bereich sind durch AntiVirus angefertigte Protokolle aufgelistet. In dem Sie auf die Spaltenüberschriften „**Startzeit**“, „**Art**“, „**Titel**“ oder „**Status**“ klicken, können Sie die vorhandenen Protokolle entsprechend sortieren.



Über doppeltes Anklicken eines Protokolls (oder das Markieren und anschließendes Anklicken von „**Öffnen**“) öffnet sich die Protokollansicht, die Sie mit den Buttons „**Speichern unter**“ und „**Drucken**“ auch als Textdatei speichern oder direkt ausdrucken können. Mit dem Auswahlfeld „**einfach / erweitert**“ können Sie festlegen, ob Informationen über Archivierte Dateien, Zugriffsverweigerungen und passwortgeschützte Archive angezeigt werden (erweitert) oder nicht (einfach). Um ein Protokoll zu löschen, markieren Sie den Tabelleneintrag mit der Maus und klicken dann bitte auf die **Entf**-Taste oder betätigen den **Löschen**-Button. .

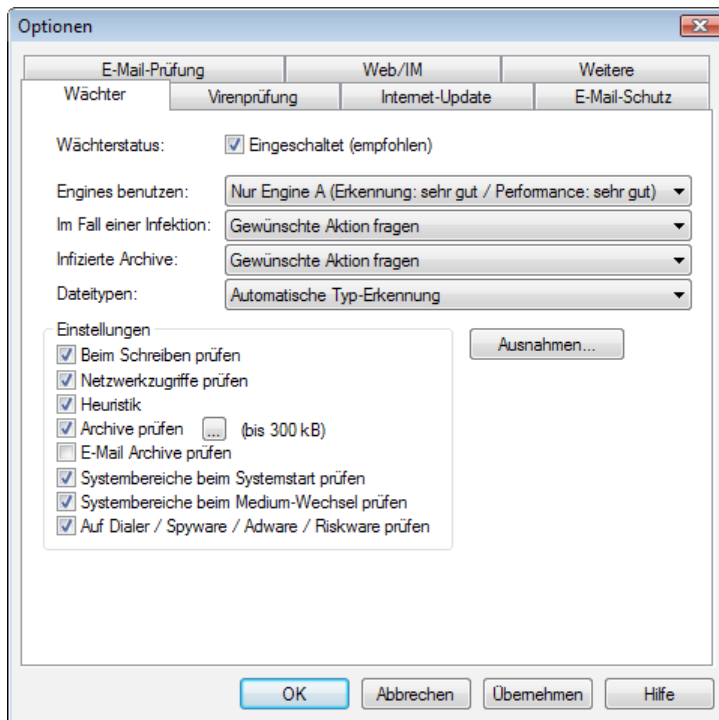
- *Generell werden nur automatische Vorgänge (automatische Virenanalyse, automatisches Update, Virenfund durch Wächter) ins Protokoll eingetragen. Wenn Sie eine direkte Virenanalyse (z.B. unter Aktionen > Rechner prüfen) ins Protokoll aufnehmen wollen, müssen Sie dieses unter „Optionen > Virenprüfung“ vorher einstellen.*

■ Optionen

Im Optionen-Bereich können Sie grundlegende Einstellungen der Software verändern. Klicken Sie dazu einfach die Registerkarte mit den jeweiligen Einstellungsoptionen an.

■ Wächter

In diesem Menü können Sie festlegen, wie die ständige Virenprüfung im Hintergrund Ihres Systems durch den Virenwächter zu erfolgen hat. Im Gegensatz zu einer Virenprüfung auf Basis eines Zeitplans oder einer manuellen Virenprüfung sollte man beim Wächter darauf achten, dass er seine Aufgaben möglichst so erledigt, ohne das System unnötig zu belasten.



- *Sollte der Virenwächter mal Alarm geschlagen haben, sollte natürlich so bald wie möglich eine ausführliche Virenprüfung erfolgen.*

■ Wächterstatus

Hier können Sie den Wächter ein- oder ausschalten. Generell sollte der Wächter natürlich eingeschaltet bleiben, nur in seltenen Ausnahmefällen macht es Sinn, den Wächter dauerhaft auszuschalten.

▣ *Um den Wächter kurzfristig auszuschalten (für einen bestimmten Zeitraum oder bis zum nächsten Systemstart), empfiehlt es sich, ihn über das Kontextmenü des Wächtersymbols in der Windows-Taskleiste auszuschalten. Auf diese Weise wird der Wächter nach der definierten Zeitspanne automatisch wieder gestartet.*

■ Engines benutzen

AntiVirus arbeitet mit zwei Antiviren-Engines, zwei grundsätzlich unabhängig voneinander operierenden Virenanalyseeinheiten. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Ergebnisse bei der Virenprophylaxe. Die Verwendung einer einzigen Engine bringt dagegen Performance-Vorteile mit sich, d.h. wenn Sie nur eine Engine verwenden, kann der Analysevorgang schneller erfolgen. In der Regel sollten Sie hier die Einstellung **„Beide Engines - performance-optimiert“** wählen, da diese die Vorteile einer doppelten Prüfung ohne größere Performance-Einbußen miteinander verbindet.

■ Im Fall einer Infektion

Hier können Sie festlegen, was bei Entdeckung einer infizierten Datei geschehen soll. Je nach dem, für welche Zwecke Sie Ihren Computer verwenden, sind hier unterschiedliche Einstellungen sinnvoll. So ist für Anwender, die viele Daten auf Ihrem Computer verwahren, die Option **„Desinfizieren (wenn nicht möglich: Zugriff sperren)“** eine empfehlenswerte Möglichkeit, da hier die Verbreitung des Virus unterbunden wird und trotzdem keine Datei auf dem Rechner gelöscht wird. Das direkte Löschen infizierter Dateien wird dagegen nur für die wenigsten Anwender sinnvoll sein. Die Nutzung des Quarantäne-Ordners über die Funktionen **„Desinfizieren (wenn nicht möglich: in Quarantäne)“** und **„Datei in Quarantäne verschieben“** bieten den Vorteil, dass die Dateien im Quarantäne-Ordner sicher verwahrt sind, ohne weiteren Schaden anrichten zu können und Sie sich später Gedanken darüber machen können, wie Sie mit den Dateien verfahren möchten.

■ Infizierte Archive

Legen Sie hier fest, ob die Behandlung von Virenfunden für Archive anders als für reguläre Dateien erfolgen soll. Da Viren innerhalb eines Archivs erst Schaden anrichten, wenn Sie entpackt werden, können Sie die Prüfung für Archive unter

Umständen unter „**Einstellungen**“ auch komplett deaktivieren. Dies bringt bei der Arbeit mit dem Wächter gewisse Performance-Verbesserungen mit sich.

So sollte man gerade die Archivdateien großer E-Mail-Postfächer nicht löschen oder in die Quarantäne verschieben, nur weil Sie in diesen eine infizierte Mail befindet. So lange der Wächter aktiv ist, können infizierte Mails auch im Postfach keinen Schaden anrichten und bei Bedarf manuell aus diesen gelöscht werden.

■ *Diese Option können Sie nicht anwählen, wenn Sie unter „Einstellungen“ das Häkchen bei „Archive prüfen“ nicht gesetzt haben.*

■ Dateitypen

Hier können Sie festlegen, welche Dateitypen von AntiVirus auf Viren untersucht werden sollen. In der Regel ist es nicht nötig, Dateien, die keinen ausführbaren Programmcode enthalten zu überprüfen. Zumal eine Überprüfung aller Dateien eines Computers durchaus eine gewisse Zeit in Anspruch nehmen kann. Wir empfehlen hier die „**automatische Typ-Erkennung**“ über die automatisch nur die Dateien geprüft werden, die theoretisch auch einen Virus enthalten können. Alternativ können Sie auch „**alle Dateien**“ überprüfen lassen. Dies dauert aber deutlich länger und ist in den seltensten Fällen angebracht.

■ *Der Unterschied zwischen „alle Dateien“ und „nur Programmdateien“ besteht darin, dass bei letzterer Funktion nur ausführbare Dateien (z.B. com, exe, bat) aber keine Archivdateien (z.B. zip, rar, tar) überprüft werden.*

■ Einstellungen

Legen Sie hier fest, welche zusätzlichen Virenanalysen AntiVirus durchführen soll. Die hier gewählten Optionen sind für sich gesehen durchaus sinnvoll, je nach Anwendungsart kann der Vorteil der Zeitersparnis durch Weglassen dieser Überprüfungen das leicht geringere Maß an Sicherheit aufwiegen.

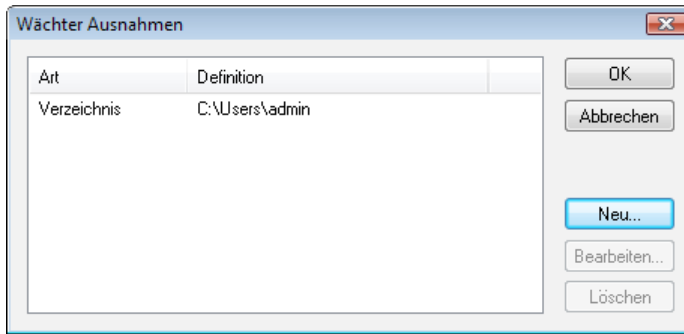
- **Beim Schreiben prüfen:** Auf diese Weise wird direkt nach dem Erzeugen einer neuen Datei geprüft, ob ein Virus sich in diesen Prozess eingeklinkt hat. Sollte ein Virus hier eingegriffen haben, wird die Aktion durchgeführt, die Sie „**im Falle einer Infektion**“ definiert haben.
- **Netzwerkzugriffe prüfen:** Wenn für Ihren Rechner eine Netzwerkverbindung zu ungeschützten Rechnern besteht (z.B. fremden Notebooks), ist es sinnvoll, auch die Netzwerkzugriffe auf die Übertragung von Schadprogrammen hin zu überprüfen. Wenn Sie Ihren Rechner als Einzelplatzrechner ohne Netzwerkzugang verwenden, muss diese Option nicht aktiviert werden. Wenn Sie auf allen Rechnern im Netzwerk einen Virenschutz installiert haben, empfiehlt es sich

ebenfalls, diese Option abzuschalten, da ansonsten manche Dateien doppelt geprüft werden, was sich negativ auf die Performance auswirkt.

- **Heuristik:** In der heuristischen Analyse werden Viren nicht nur anhand der ständig aktualisierten Virendatenbanken erkannt, sondern auch anhand bestimmter virentypischer Merkmale ermittelt. Diese Methode ist ein weiteres Sicherheitsplus, kann in seltenen Fällen aber auch einen Fehlalarm erzeugen.
- **Archive prüfen:** Das Überprüfen gepackter Daten in Archiven ist sehr zeitintensiv und kann in der Regel dann unterbleiben, wenn der Virenwächter generell auf dem System aktiv ist. Dieser erkennt dann beim Entpacken des Archives einen bis dahin verborgenen Virus und unterbindet automatisch dessen Verbreitung. Um die Performance durch das unnötige Überprüfen großer Archiv-Dateien, die selten verwendet werden, nicht zu belasten, können Sie die Größe der Archivdateien, die durchsucht werden, auf einen bestimmten Wert in Kilobyte begrenzen.
- **E-Mail Archive prüfen:** Da AntiVirus schon den Aus- und Eingang von Mails auf Virenbefall überprüft, ist es in den meisten Fällen sinnvoll, das regelmäßige Überprüfen der E-Mail-Archive zu unterlassen, da dieser Vorgang je nach Größe des Mail-Archives teilweise mehrere Minuten dauern kann.
- **Systembereiche beim Systemstart prüfen:** Systembereiche (z.B. Bootsektoren) Ihres Computers sollten in der Regel nicht von der Virenkontrolle ausgeschlossen werden. Sie können hier festlegen, ob Sie diese beim Systemstart überprüfen oder beim Medium-Wechsel (z.B. neue CD-ROM). Generell sollten Sie zumindest eine dieser beiden Funktionen aktiviert haben.
- **Systembereiche beim Medium-Wechsel prüfen:** Systembereiche (z.B. Bootsektoren) Ihres Computers sollten in der Regel nicht von der Virenkontrolle ausgeschlossen werden. Sie können hier festlegen, ob Sie diese beim Systemstart überprüfen oder beim Medium-Wechsel (neue CD-ROM o.ä.). Generell sollten Sie zumindest eine dieser beiden Funktionen aktiviert haben.
- **Auf Dialer / Spyware / Adware / Riskware prüfen:** Mit AntiVirus können Sie Ihr System auch auf Dialer und andere Schadprogramme überprüfen. Hierbei handelt es sich z.B. um Programme, die von ihnen ungewünschte teure Internetverbindungen aufbauen und in ihrem wirtschaftlichen Schadpotential dem Virus in nichts nachstehen, die z.B. Ihr Surfverhalten oder sogar sämtliche Tastatureingaben (und damit auch ihre Passwörter) heimlich speichern und bei nächster Gelegenheit übers Internet an fremde Personen weiterleiten.

■ Ausnahmen

Sie können bestimmte Laufwerke, Verzeichnisse und Dateien von der Überprüfung durch den Virenwächter ausschließen und auf diese Weise die Virenerkennung teilweise erheblich beschleunigen.



Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie auf den **Ausnahmen**-Button.
2. Klicken Sie in dem „**Wächter Ausnahmen**“-Fenster auf „**Neu...**“
3. Wählen Sie nun aus, ob Sie ein Laufwerk, ein Verzeichnis oder eine Datei bzw. einen Dateityp ausschließen möchten.
4. Wählen Sie nun mit dem Button „...“ das Verzeichnis oder das Laufwerk aus, welches Sie schützen möchten.
5. Um Dateien zu schützen, geben Sie den kompletten Dateinamen in das Eingabefeld unter „**Verzeichnis**“ ein. Sie können hier auch mit Platzhaltern arbeiten (z.B. „?“ für ein beliebiges Zeichen oder „*“ für eine beliebige Zeichenfolge).
6. Klicken Sie nun auf „**OK**“.
7. Im „**Wächter Ausnahmen**“-Fenster klicken Sie ebenfalls auf „**OK**“.

Sie können diesen Vorgang bei Bedarf beliebig oft wiederholen und im „**Wächter Ausnahmen**“-Fenster vorhandene Ausnahmen auch wieder löschen oder modifizieren.

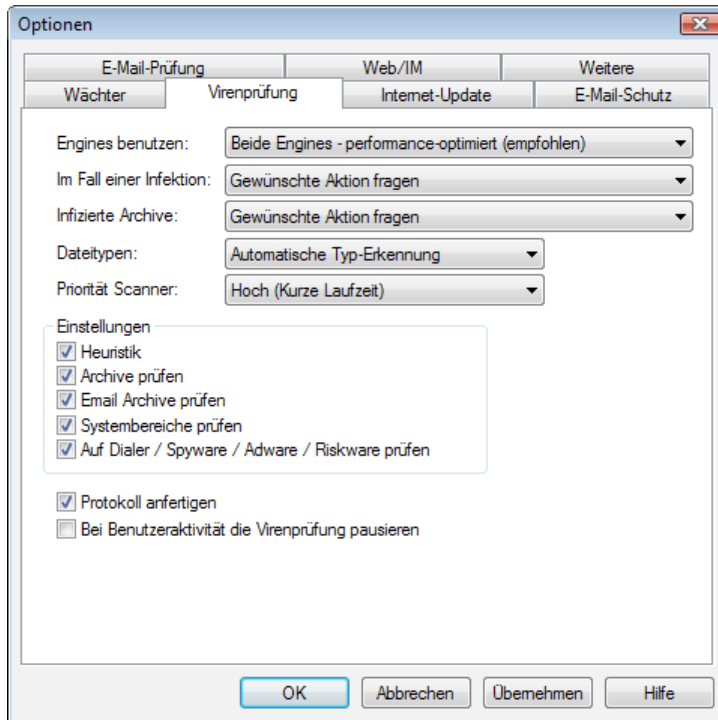
■ Die Funktionsweise von Platzhaltern ist folgendermaßen:

- ? Das Fragezeichen-Symbol ist Stellvertreter für einzelne Zeichen.
- * Das Sternchen-Symbol ist Stellvertreter für ganze Zeichenfolgen.

*Um z.B. sämtliche Dateien mit der Dateierweiterung „.exe“ prüfen zu lassen, geben Sie also *.exe ein. Um z.B. Dateien unterschiedlicher Tabellenkalkulationsformate zu überprüfen (z.B. *.xlr, *.xls), geben Sie einfach *.xl? ein. Um z.B. Dateien unterschiedlichen Typs mit einem anfänglich gleichen Dateinamen zu prüfen, geben Sie beispielsweise text*.* ein.*

■ Virenprüfung

In diesem Menü können Sie festlegen, wie die Virenprüfung durch AntiVirus zu erfolgen hat. Da eine Virenprüfung auf Basis eines Zeitplans oder eines manuellen Analysebeginns meist zu Zeiten erfolgt, in der der Computer nicht völlig mit anderen Aufgaben ausgelastet ist, können hier in der Regel mehr Systemressourcen für die Virenanalyse verwendet werden, als beim Virenwächter.



■ Engines benutzen

AntiVirus arbeitet mit zwei Antiviren-Engines, zwei grundsätzlich unabhängig voneinander operierenden Virenanalyseeinheiten. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Ergebnisse bei der Virenprophylaxe. Die Verwendung einer einzigen Engine bringt dagegen Performance-Vorteile mit sich, d.h. wenn Sie nur eine Engine verwenden, kann der Analysevorgang schneller erfolgen. In der Regel sollten Sie hier die Einstellung **„Beide Engines - performance-optimiert“** wählen, da diese die Vorteile einer doppelten Prüfung ohne größere Performance-Einbußen miteinander verbindet.

■ Im Fall einer Infektion

Hier können Sie festlegen, was bei Entdeckung einer infizierten Datei geschehen soll. Je nach dem, für welche Zwecke Sie Ihren Computer verwenden, sind hier unterschiedliche Einstellungen sinnvoll. So ist für Anwender, die viele Daten auf Ihrem Computer verwahren, die Option „**Desinfizieren (wenn nicht möglich: Zugriff sperren)**“ eine empfehlenswerte Möglichkeit, da hier die Verbreitung des Virus unterbunden wird und trotzdem keine Datei auf dem Rechner gelöscht wird. Das direkte Löschen infizierter Dateien wird dagegen nur für die wenigsten Anwender sinnvoll sein. Die Nutzung des Quarantäne-Ordners über die Funktionen „**Desinfizieren (wenn nicht möglich: in Quarantäne)**“ und „**Datei in Quarantäne verschieben**“ bieten den Vorteil, dass die Dateien im Quarantäne-Ordner sicher verwahrt sind, ohne weiteren Schaden anrichten zu können und Sie sich später Gedanken darüber machen können, wie Sie mit den Dateien verfahren möchten.

■ Infizierte Archive

Legen Sie hier fest, ob die Behandlung von Virenfunden für Archive anders als für reguläre Dateien erfolgen soll. Da Viren innerhalb eines Archivs erst Schaden anrichten, wenn Sie entpackt werden, können Sie die Prüfung für Archive unter Umständen unter „**Einstellungen**“ auch komplett deaktivieren. Dies bringt bei der Arbeit mit dem Wächter gewisse Performance-Verbesserungen mit sich. So sollte man gerade die Archivdateien großer E-Mail-Postfächer nicht löschen oder in die Quarantäne verschieben, nur weil Sie in diesen eine infizierte Mail befindet. So lange der Wächter aktiv ist, können infizierte Mails auch im Postfach keinen Schaden anrichten und bei Bedarf manuell aus diesen gelöscht werden.

■ Dateitypen

Hier können Sie festlegen, welche Dateitypen von AntiVirus auf Viren untersucht werden sollen. In der Regel ist es nicht nötig, Dateien, die keinen ausführbaren Programmcode enthalten zu überprüfen. Zumal eine Überprüfung aller Dateien eines Computers durchaus eine gewisse Zeit in Anspruch nehmen kann. Wir empfehlen hier die „**automatische Typ-Erkennung**“ über die automatisch nur die Dateien geprüft werden, die theoretisch auch einen Virus enthalten können. Alternativ können Sie auch „**alle Dateien**“ überprüfen lassen. Dies dauert aber deutlich länger und ist in den seltensten Fällen angebracht.

□ *Der Unterschied zwischen „alle Dateien“ und „nur Programmdateien“ besteht darin, dass bei letzterer Funktion nur ausführbare Dateien (z.B. com, exe, bat) aber keine Archivdateien (z.B. zip, rar, tar) überprüft werden.*

■ **Priorität Scanner**

Über diese Einstellung können Sie bestimmen, wie viele Systemressourcen von AntiVirus für eine Virenprüfung genutzt werden sollen. Wenn während der Virenprüfung auf dem Rechner noch gearbeitet werden soll, empfehlen wir die Einstellung „**Niedrig (Lange Laufzeit)**“. Bei einem momentan nicht benutzten Rechner die Einstellung „**Hoch (Kurze Laufzeit)**“.

■ *Beachten Sie in diesem Zusammenhang bitte auch die Funktion „Bei Benutzeraktivität die Virenprüfung pausieren“, die weiter unten erläutert wird.*

■ **Einstellungen**

Legen Sie hier fest, welche zusätzlichen Virenanalysen AntiVirus durchführen soll. Die hier gewählten Optionen sind für sich gesehen durchaus sinnvoll, je nach Anwendungsart kann der Vorteil der **Zeitersparnis** durch Weglassen dieser Überprüfungen das leicht geringere Maß an Sicherheit aufwiegen.

- **Heuristik:** In der heuristischen Analyse werden Viren nicht nur anhand der ständig aktualisierten Virendatenbanken erkannt, sondern auch anhand bestimmter virentypischer Merkmale ermittelt. Diese Methode ist ein weiteres Sicherheitsplus, kann in seltenen Fällen aber auch einen Fehlalarm erzeugen.
- **Archive prüfen:** Das Überprüfen gepackter Daten in Archiven ist sehr zeitintensiv und kann in der Regel dann unterbleiben, wenn der Virenwächter generell auf dem System aktiv ist. Dieser erkennt dann beim Entpacken des Archives einen bis dahin verborgenen Virus und unterbindet automatisch dessen Verbreitung. Um die Performance durch das unnötige Überprüfen großer Archiv-Dateien, die selten verwendet werden, nicht zu belasten, können Sie die Größe der Archivdateien, die durchsucht werden, auf einen bestimmten Wert in Kilobyte begrenzen.
- **E-Mail Archive prüfen:** Da AntiVirus schon den Aus- und Eingang von Mails auf Virenbefall überprüft, ist es in den meisten Fällen sinnvoll, das regelmäßige Überprüfen der E-Mail-Archive zu unterlassen, da dieser Vorgang je nach Größe des Mail-Archives teilweise mehrere Minuten dauern kann.
- **Systembereiche prüfen:** Systembereiche (z.B. Bootsektoren) Ihres Computers sollten in der Regel nicht von der Virenkontrolle ausgeschlossen werden.
- **Auf Dialer / Spyware / Adware / Riskware prüfen:** Mit AntiVirus können Sie Ihr System auch auf Dialer und andere Schadprogramme überprüfen. Hierbei handelt es sich z.B. um Programme, die von ihnen ungewünschte teure Internetverbindungen aufbauen und in ihrem wirtschaftlichen Schadpotential dem Virus in nichts nachstehen, die z.B. Ihr Surfverhalten oder sogar sämtliche Tastatureingaben (und damit auch ihre Passwörter) heimlich speichern und bei nächster Gelegenheit übers Internet an fremde Personen weiterleiten.

■ Protokoll anfertigen

Über das Häkchenfeld „**Protokoll anfertigen**“ können Sie festlegen, dass AntiVirus über den Virenprüfungsvorgang ein Protokoll anlegt. Dies kann dann im Protokoll-Bereich eingesehen werden. Wenn Sie das Häkchen hier nicht setzen, werden weiterhin nur automatische Vorgängen (automatische Virenanalyse, automatisches Update, Virenfund durch Wächter) im Protokoll eingetragen.

■ Bei Benutzeraktivität die Virenprüfung pausieren

Mit dieser Funktion können Sie interaktiv auf die Auslastung Ihres Rechners reagieren. Sobald er vom Anwender für die Arbeit mit Programmen genutzt wird, wird die systematische Virenprüfung angehalten. Die ständige Hintergrundkontrolle vom Wächter wird hierbei natürlich nicht beeinträchtigt. Wenn der Rechner dann nicht benutzt wird, wird die Arbeitspause gezielt dazu genutzt, die systematische Virenprüfung voranzutreiben.

☐ *Wenn Sie diese Funktion aktivieren, ist es natürlich empfehlenswert, unter „Priorität Scanner“ die Einstellung „Hoch“ zu verwenden. So kann die Virenkontrolle bei der Nichtnutzung des Computers um so schneller erfolgen.*

■ Internet-Update

Geben Sie hier die Zugangsdaten (Benutzername und Passwort) ein, die Sie bei der Anmeldung von AntiVirus erhalten haben. Mit Hilfe dieser Daten werden Sie vom G DATA-Server erkannt und das Update der Virensignaturen kann vollautomatisch erfolgen.

☐ *Generell geben Sie die Zugangsdaten gleich beim ersten Start von AntiVirus ein und die Software merkt sich diese Einstellungen. Im Bereich „**Optionen > Internet-Update**“ müssen Sie eigentlich nur Änderungen vornehmen, wenn Sie die Software nach einer Deinstallation erneut installieren oder sich die Einstellungen Ihres Internet-Zugangs verändert haben.*

■ Am Server anmelden

Wenn Sie noch keine Anmeldung am Server durchgeführt haben, können Sie diese jetzt nachholen, indem Sie auf den Button „**Am Server anmelden**“ klicken. Es erscheint ein Eingabefenster, in dem Sie ihre **Registriernummer** und **Kundendaten** eingeben.

☐ *Sollte das AntiVirus keine Verbindung mit dem Internet aufnehmen können, klicken Sie bitte auf den Erweitert-Button und nehmen die notwendigen Internet-Einstellungen vor.*

- Die Registriernummer finden Sie auf der Rückseite des gedruckten Bedienungshandbuches. Wenn Sie die Software online gekauft haben, erhalten Sie die Registrierungsnummer in einer gesonderten E-Mail.

Klicken Sie nun auf den **Anmelden**-Button und Ihre Zugangsdaten werden auf dem G DATA-Updateserver generiert. Wenn die Anmeldung erfolgreich verlief, erscheint ein Info-Bildschirm mit dem Vermerk „**Die Anmeldung wurde erfolgreich durchgeführt**“, den Sie mit dem **Schließen**-Button verlassen können.

Achtung: Für Ihre Unterlagen und für etwaige Neuinstallationen der Software erhalten Sie Ihre Zugangsdaten auch per Mail zugesickt. Bitte vergewissern Sie sich deshalb, dass Ihre in der Online-Registrierung angegebene E-Mail-Adresse korrekt ist; ansonsten stehen Ihnen die Zugangsdaten nicht zur Verfügung.

Abschließend werden die Zugangsdaten automatisch in die ursprüngliche Eingabemaske übernommen und Sie können durch Anklicken des **OK**-Buttons den eigentlichen Update-Vorgang starten.

- Sie können das Update auch jederzeit nachträglich durchführen.

■ Internet-Einstellungen

Falls Sie einen Rechner hinter einer **Firewall** verwenden oder andere besondere Einstellungen bezüglich Ihres Internetzugangs haben, verwenden Sie bitte einen **Proxyserver**. Sie sollten diese Einstellung nur ändern, wenn das Internet-Update nicht funktioniert. Wenden Sie sich wegen der Proxy-Adresse gegebenenfalls an Ihren Systemadministrator oder Internetzugangsanbieter. Die Zugangsdaten für die Internetverbindung (Benutzernamen und Passwort) sind gerade beim automatischen Internet-Update per Zeitplan sehr wichtig. Ohne diese Angaben kann keine automatische Verbindung mit dem Internet erfolgen. Achten Sie bitte auch darauf, dass Sie in Ihren allgemeinen Interneteinstellungen (z.B. für Ihr Mailprogramm oder Ihren Internetbrowser) die automatische Einwahl ermöglichen. Ohne die automatische Einwahl startet AntiVirus zwar den Internet-Update-Vorgang, muss dann aber darauf warten, dass Sie den Aufbau der Internetverbindung mit „**OK**“ bestätigen.

■ Versionsprüfung

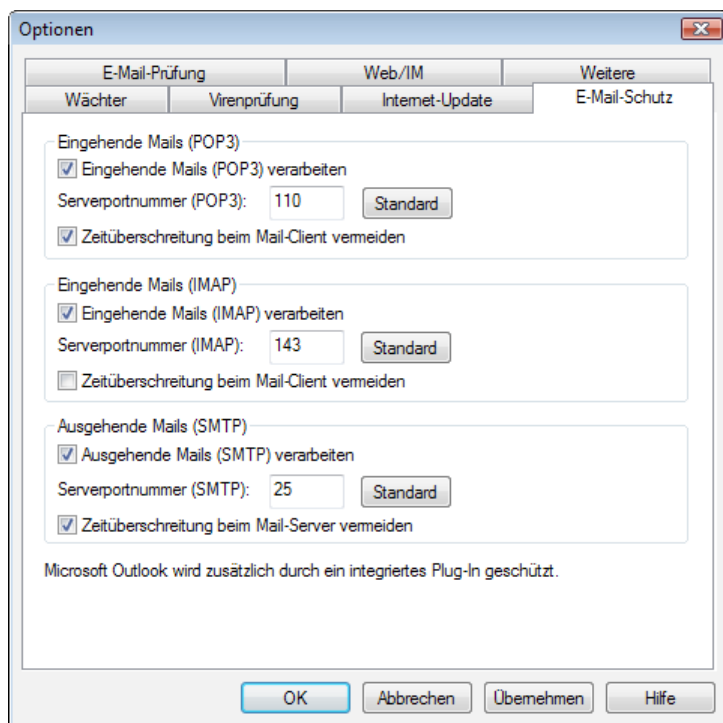
Die Versionsprüfung sollten Sie nur dann deaktivieren, wenn es Probleme mit den Virensignaturen gibt (z.B. weil Sie versehentlich hier Dateien gelöscht haben). Bei ausgeschalteter Versionsprüfung dauert das Update etwas länger, weil für alle Dateien eine Prüfsumme berechnet wird und diese mit der Prüfsumme auf dem Server verglichen wird.

■ E-Mail-Schutz

AntiVirus schützt nach der Installation automatisch auch Ihre E-Mails. Dazu verwendet es für Microsoft Outlook ein spezielles PlugIn und für POP3/IMAP basierte E-Mail-Programme (wie z.B. Outlook Express, Thunderbird, Pegasus, Opera etc.) einen speziellen Client, der die Mails überprüft, bevor Sie von Ihrem E-Mail-Programm empfangen bzw. versendet werden. Durch Setzen der jeweiligen Häkchen können Sie den Schutz für eingehende Mails (POP3/IMAP) und ausgehende Mails (SMTP) auch abschalten.

☐ Wenn Sie bei der Nutzung Ihrer E-Mail-Programme nicht die Standardports verwenden, können Sie unter „**Serverportnummer**“ auch den **Port** angeben, den Sie für eingehende oder ausgehende Mails verwenden. Mit Anklicken des **Standard**-Buttons können Sie automatisch die Standardportnummern wiederherstellen.

☐ Microsoft Outlook wird durch ein spezielles PlugIn geschützt, mit dem Sie direkt aus **Outlook** heraus Ordner und Mails überprüfen können. Um in Outlook eine E-Mail oder einen Ordner auf Viren zu überprüfen, wählen Sie einfach in der Outlook-Menüleiste den Befehl „**Extras > Ordner auf Viren überprüfen**“. und der aktuell ausgewählte Mailordner wird auf Viren überprüft.

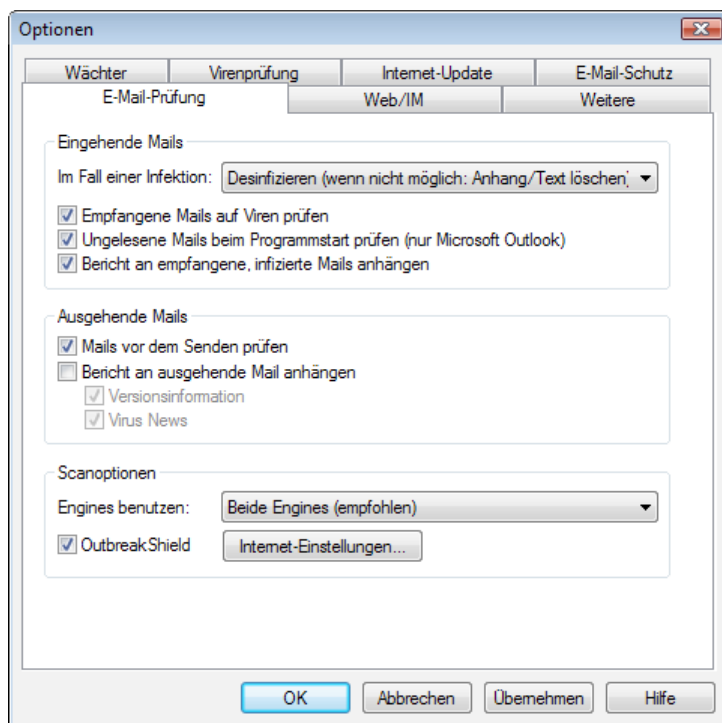


■ Zeitüberschreitung beim Mail-Programm vermeiden

Da AntiVirus die eingehenden Mails zeitlich vor dem eigentlichen Mailprogramm bearbeitet, kann es bei großen Mail-Mengen oder langsamen Verbindungen vorkommen, dass eine Fehlermeldung beim Mailprogramm erscheint, weil es nicht sofort die Maildaten zugestellt bekommt, da diese ja von AntiVirus auf Viren überprüft werden. Mit Aktivieren dieses Häkchenfeldes wird eine solche Fehlermeldung des Mailprogramms unterdrückt und sobald sämtliche Maildaten auf Viren überprüft wurden, werden diese von AntiVirus dann ganz normal an das Mailprogramm überreicht.

■ E-Mail-Prüfung

Mit der E-Mail-Prüfung können Sie ein- und ausgehende E-Mails und deren Dateianhang auf Viren überprüfen und mögliche Infektionen direkt an der Quelle ausschalten. AntiVirus ist in der Lage, bei Virenfund Dateianhänge direkt zu löschen oder infizierte Dateien zu reparieren.



■ In Microsoft Outlook wird die E-Mail-Prüfung durch ein PlugIn realisiert. Dieses bietet denselben Schutz wie die POP3/IMAP orientierte Schutzfunktion innerhalb der AntiVirus-Optionen. Nach der Installation dieses PlugIns (erfolgt auf Wunsch automatisch bei der Installation von AntiVirus) finden Sie im Menü „Extras“ die Funktion „Ordner auf Viren prüfen“, mit der Sie Ihre Mailordner einzeln auf Virenbefall checken können.

■ Im Fall einer Infektion

Hier können Sie festlegen, was bei Entdeckung einer infizierten Mail geschehen soll. Je nachdem, für welche Zwecke Sie Ihren Computer verwenden, sind hier unterschiedliche Einstellungen sinnvoll. In der Regel ist die Einstellung **„Desinfizieren (wenn nicht möglich: Anhang/Text löschen)“** empfehlenswert.

■ Empfangene Mails auf Viren prüfen

Mit Aktivierung dieser Option werden sämtliche E-Mails auf Viren überprüft, die Sie während Ihrer Arbeit am Computer erreichen.

■ Ungelesene Mails beim Programmstart prüfen

Nur für Microsoft Outlook: Diese Option dient dazu, E-Mails auf Virenbefall zu kontrollieren, die Sie erreichen, während Sie nicht mit dem Internet verbunden sind. Sobald Sie Outlook starten, werden deshalb sämtliche ungelesenen Mails im Posteingang-Ordner und den darin enthaltenen Unterordnern von AntiVirus kontrolliert.

■ Bericht an empfangene, infizierte Mails anhängen

Wenn Sie die Berichtsoption aktiviert haben, erscheint im Fall eines Virenfundes in der Betreffzeile der infizierten Mail die Warnung [**VIRUS**] und am Anfang des Mailtextes die Mitteilung „**ACHTUNG! Diese Mail enthält folgenden Virus:**“ gefolgt vom Namen des Virus und der Angabe, ob der Virus gelöscht oder die infizierte Datei repariert werden konnte.

■ Mails vor dem Senden prüfen

Damit Sie nicht versehentlich selber Viren verschicken, bietet AntiVirus auch die Möglichkeit, Ihre Mails vor dem Versenden auf Virenbefall zu überprüfen. Sollten Sie tatsächlich einen Virus versenden wollen, erscheint die Meldung „**Die Mail [Betreffzeile] enthält folgenden Virus: [Virusname] Die Mail kann nicht verschickt werden**“ und die entsprechende E-Mail wird nicht versandt.

■ Bericht an ausgehende Mails anhängen

Ein Prüfbericht wird im Body jeder ausgehenden E-Mail unter dem eigentlichen Mailtext angezeigt. Sie können hier außerdem festlegen, ob dieser Bericht Informationen über die verwendete AntiVirus-Version („**Versionsinformation**“) und einen Internet-Link zum „**AntiVirusLab**“ enthält („**Virus News**“), in dem Anwender online ständig aktualisierte Informationen über Viren erhalten können. Ein kompletter Bericht würde also in etwa folgendermaßen aussehen:

Virus checked by G DATA AntiVirus

Version: GDAV 15.0.37 from 06.10.2007

Virus news: www.antiviruslab.com

■ Engines benutzen

AntiVirus arbeitet mit zwei Antiviren-Engines, zwei grundsätzlich unabhängig voneinander operierenden Virenanalyseeinheiten. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Ergebnisse bei der Virenprophylaxe.

■ OutbreakShield

Hiermit aktivieren Sie das OutbreakShield. AntiVirus erstellt bei aktiviertem OutbreakShield Prüfsummen von Mails, gleicht diese im Internet mit stets aktualisierten Anti-Spam-Blacklists ab und ist dadurch in der Lage, auf ein Massenmailing zu reagieren, bevor entsprechende Virensignaturen zur Verfügung stehen.

■ *Falls Sie einen Rechner hinter einer Firewall verwenden oder andere besondere Einstellungen bezüglich Ihres Internetzugangs haben, verwenden Sie bitte einen Proxyserver. Klicken Sie dazu auf den Button „Internet-Einstellungen“ und nehmen die entsprechenden Änderungen vor. Sie sollten diese Einstellung nur ändern, wenn das OutbreakShield nicht funktioniert. Wenden Sie sich wegen der Proxy-Adresse gegebenenfalls an Ihren Systemadministrator oder Internetzugangsanbieter.*

■ Web / IM

■ Internetinhalte (HTTP)

In den Web-Optionen können Sie bestimmen, dass sämtliche **HTTP-Webinhalte** schon beim Browsen auf Viren überprüft werden. Infizierte Webinhalte werden dann gar nicht erst ausgeführt und die entsprechenden Seiten nicht angezeigt. Setzen Sie hierzu bitte das Häkchen bei „**Internetinhalte (HTTP) verarbeiten**“.

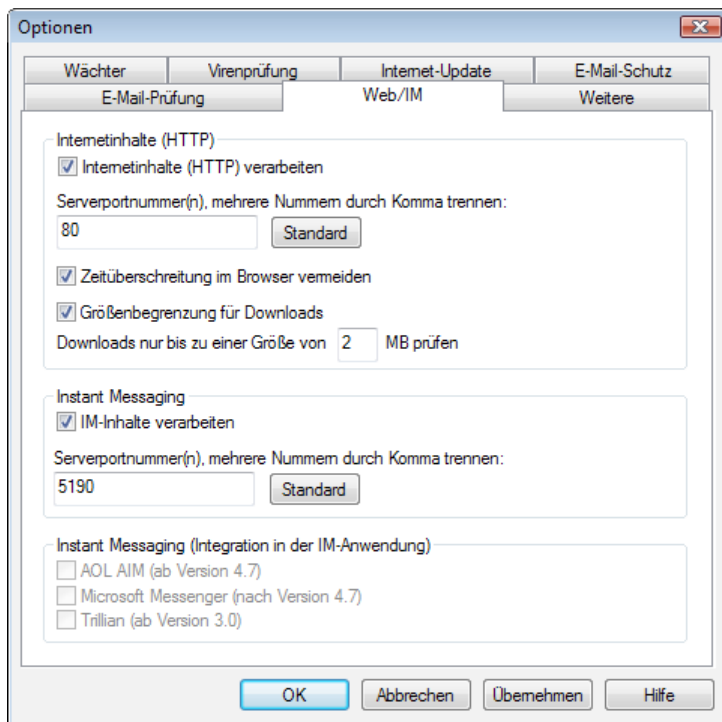
■ *Wenn Sie die Internetinhalte nicht prüfen lassen wollen, greift natürlich der Virenwächter dann ein, wenn infizierte Dateien zur Ausführung geraten. Ihr System ist also auch ohne die Überprüfung von Internetinhalten geschützt, solange der Virenwächter aktiviert ist. Sollten Sie AntiVirus jedoch zusammen mit der G DATA Kindersicherung und dem Webfilter verwenden wollen (z.B. im Rahmen des G DATA InternetSecurity-Pakets), muss das Häkchen bei „Internetinhalte (HTTP) verarbeiten“ gesetzt sein, da sonst Kindersicherung und Webfilter nicht korrekt funktionieren.*

Da AntiVirus die Web-Inhalte vor Ihrer Darstellung im Internet Browser bearbeitet und dafür je nach Datenaufkommen eine gewisse Zeit benötigt, kann es vorkommen, dass eine Fehlermeldung im Internet Browser erscheint, weil dieser nicht sofort die Daten zugestellt bekommt, da diese ja von AntiVirus auf Schadroutinen überprüft werden. Mit Aktivieren des Häkchenfeldes „**Zeitüberschreitung im Browser vermeiden**“ wird eine solche **Fehlermeldung** unterdrückt und sobald sämtliche Browserdaten auf Viren überprüft wurden, werden diese von AntiVirus dann ganz normal an den Internetbrowser überreicht.

Mit der „**Größenbegrenzung für Downloads**“ können Sie die HTTP-Überprüfung für zu große Webinhalte unterbrechen. Die Inhalte werden dann vom

Virenwächter überprüft, sobald etwaige Schadroutinen aktiv werden. Der Vorteil bei dieser Größenbegrenzung liegt darin, dass es beim Surfen im Web nicht zu Verzögerungen durch die Virenkontrolle kommt.

- *Inhalte, die wegen Ihrer Größe nicht VOR Ihrer Anzeige im Browser auf Viren und Schadprogramme überprüft werden, werden vom Wächter natürlich spätestens dann erkannt und geblockt, wenn sie Schadroutinen ausführen möchten.*



■ Instant Messaging

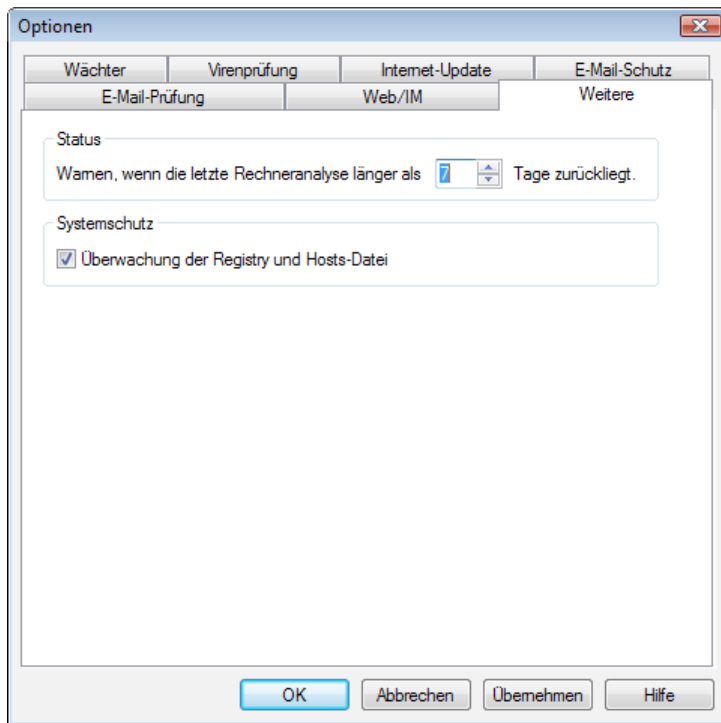
Da auch über Instant Messaging-Tools Viren und andere Schadprogramme verbreitet werden können, kann AntiVirus auch hier die Anzeige und den Download infizierter Daten im Vorfeld unterbinden. Sollten Ihre Instant Messaging-Anwendungen nicht über die Standardportnummern ablaufen, geben Sie bitte unter „**Serverportnummer**“, die entsprechenden **Port-Adressen** ein.

■ Instant Messaging (Integration in der IM-Anwendung)

Sollten Sie **AOL AIM (ab Version 4.7)**, den **Microsoft Messenger (ab Version 4.7)** oder **Trillian (ab Version 3.0)** verwenden, können Sie durch Setzen des Häkchens für das jeweilige Programm ein Kontextmenü definieren, in dem Sie verdächtige Dateien direkt auf Viren überprüfen können.

■ Weitere

Hier stehen Ihnen weitere Optionen für Ihr AntiVirus zur Verfügung.



■ Status

Hier können Sie festlegen, wann AntiVirus im **Status-Bereich** ein warnendes Achtung-Symbol an Stelle des grünen Häkchensymbols zeigen soll. Geben Sie dazu bei „**Warnen, wenn die letzte Rechneranalyse länger als ___ Tage zurückliegt**“ einen für Ihre Bedürfnisse realistischen Wert ein (z.B. sieben Tage). Auf diese Weise haben Sie die Aktualität Ihrer Virenprophylaxe immer im Blick und können diese an individuelle Bedürfnisse anpassen.

■ *Neben der ständigen Virenanalyse Ihres Computers über den Virenwächter sollten Sie auch regelmäßig eine „große“ Virenkontrolle vornehmen. Generell empfiehlt es sich, eine Virenprüfung spätestens dann durchzuführen, wenn Sie neue Virensignaturen über das Internet-Update erhalten haben. Selbstverständlich können Sie die Rechneranalyse auch automatisieren.*

■ **Systemschutz**

Wenn der Systemschutz aktiviert ist, werden bei jedem Systemstart die Windows-Registry und die Systemordner überprüft. Auf diese Weise wird die HOSTS-Datei vor Manipulationen geschützt.

■ *Die HOSTS-Datei ist eine Textdatei auf Ihrem Rechner, die Hostnamen mit den IP-Adressen abgleicht. Wird diese durch Schadprogramme modifiziert, können Anwender ungewollt z.B. auf Phishing-Websites umgeleitet werden.*

■ Erste Schritte

Eine **Firewall** dient dazu, Ihren Rechner vor Angriffen aus dem Internet zu schützen und ihre vertraulichen Daten vor Missbrauch zu bewahren. Eine gut konfigurierte Firewall macht Ihren Rechner im Internet für Hacker quasi unsichtbar und im Zusammenspiel mit einer aktuellen Antivirensoftware können Sie Ihren Computer bestmöglich vor Fremdeinflussnahme schützen.



Sobald die Firewall installiert ist, verfolgt sie sämtliche **Netzwerkaktivitäten** Ihres Computers. Wenn Sie mit Ihrem Computer lokal arbeiten, fällt die Firewall nur durch das **Security-Symbol** in der Start-Leiste von Windows auf. Hierauf können Sie durch einen Klick mit der **rechten Maustaste** ein **Kontextmenü** öffnen, in dem Sie sich eine **Statistik** anzeigen lassen und die Programmoberfläche der Firewall öffnen. Welche Funktionen Sie im einzelnen über das **Security-Symbol** aufrufen können, erfahren Sie in dem Kapitel „**Security-Symbol**“.

Sobald die Firewall auf Ihrem Computer eine Anfrage ans Netzwerk bzw. Internet registriert, erscheint eine **Info-Box**, in der Sie entscheiden können, ob Sie dem jeweiligen Programm den Netzwerkzugriff erlauben oder verbieten. Welche Einstellungen hier möglich sind, lesen Sie im Kapitel „**Firewall-Alarm**“.



Die Firewall ist auf diese Weise **selbstlernend**, merkt sich (sobald Sie eine „**dauerhafte Regel**“ erstellen), die von Ihnen vorgenommenen Einstellungen und passt sich so an Ihr Anwenderverhalten an. Selbstverständlich können Sie über die Firewall-Programmoberfläche auch alle über die Info-Boxen erstellten Regeln für Programme rückgängig machen oder ändern.

- *Generell sollten Sie den Zugriff aufs Netzwerk oder Internet nur Programmen erlauben, die Ihnen bekannt sind und bei denen Sie wissen, wieso hier eine Verbindung aufgebaut werden soll.*
- *Manche Schadprogramme verwenden dieselben Namen wie andere unbedenkliche Programme. Sie sollten hier generell achtsam sein.*

■ Bedienung der Software

Die Bedienung der Firewall ist prinzipiell selbsterläuternd und übersichtlich gestaltet. Anhand unterschiedlicher **Karteikarten**, die Sie über die links in der Firewall angezeigten Symbole anwählen können, wechseln Sie in den jeweiligen Programmbereich und können dort Aktionen durchführen, Voreinstellungen vornehmen oder Verbindungsdetails überprüfen.



Folgende **Programmbereiche** stehen Ihnen zur Verfügung und werden Ihnen in den gleichnamigen Kapiteln dieser Bedienungsanleitung ausführlich erläutert.

- Status-Bereich
- Netzwerke-Bereich
- Regelsätze-Bereich
- Anwendungen-Bereich
- Verbindungen-Bereich

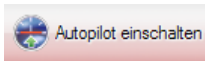
Außerdem finden Sie in der oberen **Menüleiste** der Firewall-Programmoberfläche übergreifende Funktionen und Einstellungsmöglichkeiten sowie das Security-Symbol in der Taskleiste Ihres Desktop (in der Regel unten rechts neben der Windows-Systemuhr).

■ Menüleiste

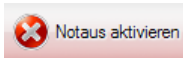
In der Menüleiste stehen Ihnen folgende Funktionen zur Auswahl:



Über das Optionen-Menü können Sie grundlegende Einstellungen und Vorgaben für die Arbeit mit der Firewall vornehmen. Die jeweiligen Bereiche werden Ihnen ausführlich in dem Kapitel „**Optionen**“ erläutert.



Hier können Sie den Autopiloten ein- oder ausschalten, der z.B. die Nutzung von Online-Spielen erleichtert.



Wenn Sie den Eindruck haben, dass ganz aktuell ein Angriff auf Ihren Computer erfolgt oder Sie z.B. das Gefühl haben, dass sich gerade ein Dialer gegen Ihren Willen verbinden will, können Sie mit dem **Notaus**-Button den Zugriff Ihres Computers auf das Netzwerk vollständig blockieren. Dieser Modus entspricht der physikalischen Trennung des Computers vom Internet und/oder vom lokalen Netzwerk.



Hiermit rufen Sie die Online-Hilfe auf.

■ Programmbereiche

■ Status-Bereich

Im **Status-Bereich** der Firewall erhalten Sie grundlegende Informationen zum aktuellen Zustand Ihres Systems und der Firewall. Diese finden sich rechts vom jeweiligen Eintrag als Text- oder Zahlenangabe. Darüber hinaus wird der Status der Komponenten auch grafisch dargestellt:



Ein grünes **Häkchen** weist darauf hin, dass die jeweilige Komponente aktiv ist und ihre Schutzfunktion erfüllt.



Ein **Verbotsschild** informiert darüber, dass die entsprechende Komponente nicht aktiv ist und die jeweilige Schutzfunktion nicht zur Verfügung steht.

■ *Wenn sich die Firewall-Programmoberfläche öffnet, sind für kurze Zeit die meisten Symbole im Achtung-Modus. Das heißt nicht, dass die Firewall Ihren Computer in diesem Moment nicht schützt. Hier handelt es sich ganz im Gegenteil um eine interne Überprüfung des Status, die Ihnen anzeigt, dass hier ein automatischer Check der Funktionen erfolgt.*

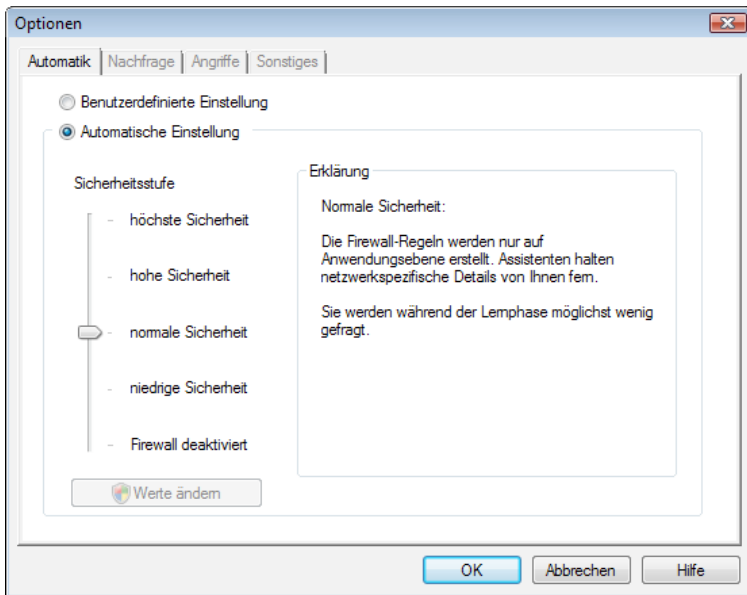


Durch doppeltes Anklicken des jeweiligen Eintrags (oder durch Auswählen des Eintrags und Anklicken des **Bearbeiten**-Buttons) können Sie hier direkt Aktionen

vornehmen oder in den jeweiligen Programmbereich wechseln. Sobald Sie die Einstellungen einer Komponente mit **Achtung**-Symbol optimiert haben, wechselt das Symbol im Status-Bereich wieder auf das grüne Häckchensymbol.

■ Sicherheit

Während Sie den Computer für ihre tägliche Arbeit nutzen, lernt die Firewall nach und nach, welche Programme Sie für den Zugang zum Internet nutzen, welche nicht und welche Programme ein Sicherheitsrisiko sind. Je nach dem, wie sehr sie sich in der Materie der Firewall-Technologie auskennen, können Sie die Firewall so **konfigurieren**, dass Sie Ihnen entweder einen sehr guten **Basis-Schutz** bietet, ohne viele Nachfragen zu stellen oder aber einen professionellen Schutz, der sich sehr genau an ihrem **Computernutzungsverhalten** ausrichtet, aber auch gewisse Kenntnisse von Ihnen als Anwender verlangt.



Wenn Sie einen Doppelklick mit der Maus auf den Eintrag „**Sicherheit**“ ausführen, haben Sie eine Auswahl aus folgenden **Sicherheitsvarianten**:

- **Höchste Sicherheit:** Die Firewall-Regeln werden mit sehr feinkörnigen Richtlinien erstellt. Dazu sollten Sie sich mit netzwerkspezifischen Fachbegriffen auskennen (TCP, UDP, Ports etc.). Die Firewall bemerkt kleinste Ungereimtheiten und wird während der Lernphase sehr häufig nachfragen.

- **Hohe Sicherheit:** Die Firewall-Regeln werden mit sehr feinkörnigen Richtlinien erstellt. Dazu sollten Sie sich mit netzwerkspezifischen Fachbegriffen auskennen (TCP, UDP, Ports etc.). Die Firewall wird während der Lernphase unter Umständen häufig nachfragen.
- **Normale Sicherheit:** Die Firewall-Regeln werden nur auf Anwendungsebene erstellt. Assistenten halten netzwerkspezifische Details von Ihnen fern. Sie werden während der Lernphase möglichst wenig gefragt.
- **Niedrige Sicherheit:** Die Firewall-Regeln werden nur auf Anwendungsebene erstellt. Assistenten halten netzwerkspezifische Details von Ihnen fern und Sie werden während der Lernphase selten gefragt. Höchst sicherer Schutz vor ankommenden Verbindungsanforderungen besteht auch in dieser Sicherheitsstufe.
- **Firewall deaktiviert:** Sie können die Firewall bei Bedarf auch abschalten. Ihr Computer ist dann weiterhin mit dem Internet und anderen Netzwerken verbunden, wird von der Firewall aber nicht mehr vor Angriffen oder Spionage-Attacken geschützt.

Benutzerdefinierte Einstellungen

Sie können die Firewall auch direkt manuell konfigurieren. Wenn Sie das Häkchen bei „**Benutzerdefinierte Einstellungen**“ setzen erscheinen oben rechts weiter Registerreiter mit denen Sie die Firewall ganz nach Ihren Wünschen einstellen können. Eine ausführliche Erläuterung zu den Karteireitern und ihren Einstellungsmöglichkeiten finden Sie im Kapitel „**Optionen**“ und dessen Unterkapiteln.

■ Netzwerke

Die Firewall überwacht natürlich sämtliche Netzwerkaktivitäten, wie z.B. ein **DFÜ-Netzwerk** und eine **Local Area Connection**. Sollten ein oder mehrere Netzwerke nicht geschützt werden, weil sie z.B. manuell von der Firewallüberwachung ausgenommen wurden, weist Sie ein Achtung-Symbol darauf hin. Ein Doppelklick auf diesen Eintrag führt Sie in den Netzwerke-Bereich der im Kapitel „**Programmbereiche** > **Netzwerk-Bereich**“ ausführlich erläutert wird.

■ *Neue Netzwerkverbindungen werden von der Firewall natürlich automatisch erkannt. Sobald ein neues Netzwerk sich installiert hat, werden Sie gefragt, welchen Regelsatz (also vertrauenswürdiges Netzwerk, nicht vertrauenswürdiges Netzwerk oder zu blockierendes Netzwerk) Sie für dieses Netzwerk verwenden möchten.*

■ Ausgehende Verbindungen

Unter **“Ausgehende Verbindungen”** wird Ihnen angezeigt, wie viele **Verbindungen** Ihr Computer aktuell mit dem Netzwerk bzw. Internet bestehen hat. Wenn Sie auf diese Anzeige klicken, gelangen Sie in den Anwendungen-Bereich und erhalten dort genaue Informationen zu diesen Verbindungen. Lesen Sie hierzu bitte das Kapitel **„Anwendungen-Bereich“**.

■ Eingehende Verbindungen

Unter **“Eingehende Verbindungen”** wird Ihnen angezeigt, wie viele **Verbindungen** Ihr Computer aktuell mit dem Netzwerk bzw. Internet bestehen hat. Wenn Sie auf diese Anzeige klicken, gelangen Sie in den Anwendungen-Bereich und erhalten dort genaue Informationen zu diesen Verbindungen. Lesen Sie hierzu bitte das Kapitel **„Anwendungen-Bereich“**.

■ Unbekannte Server-Anwendungen

Die Firewall erkennt Anwendungen, die auf eingehenden Verbindungen “lauschen” als **“unbekannte Server-Anwendungen”**. Diese Anwendungen müssen nicht zwangsläufig ein Sicherheitsrisiko darstellen. Sollten von der Firewall unbekannte **Server-Anwendungen** entdeckt werden, sollten Sie für die jeweilige Anwendung eine spezielle Regel definieren. Dies können Sie erreichen, indem Sie auf den Eintrag **„Unbekannte Server-Anwendungen“** klicken.

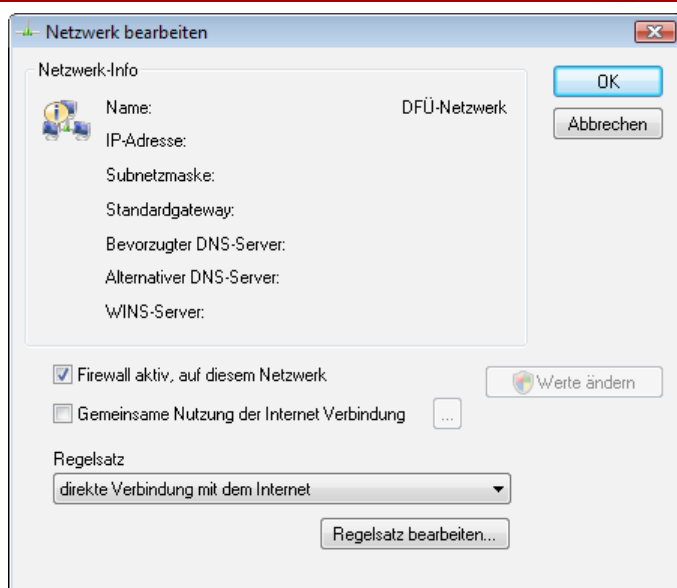
☐ *Wenn keine unbekannten Server-Anwendungen vorliegen, bringt Sie ein Anklicken dieses Eintrags in den Bereich „Anwendungen“.*

■ Ungelesene Nachrichten

Über diesen Eintrag können Sie sich die **Systemnachrichten** der Firewall anzeigen lassen. Sobald neue, ungelesene Nachrichten bereitstehen, weist Sie ein Achtung-Symbol darauf hin. Klicken Sie einfach mit der Maus auf den Eintrag und Sie gelangen in den Bereich für die Systemnachrichten. Dort können Sie sich die Nachrichten anzeigen lassen und ggf. abspeichern und/oder ausdrucken.

■ Netzwerke-Bereich

Im **Netzwerke-Bereich** werden die Netzwerke (z.B. **LAN**, **DFÜ** etc.) aufgelistet, mit denen ihr Rechner verbunden ist. Hier wird auch aufgezeigt, nach welchem Regelsatz (siehe Kapitel **„Regelsätze-Bereich“**) das jeweilige Netzwerk geschützt wird. Wenn Sie das Häkchen vor dem jeweiligen Netzwerk entfernen, wird dieses vom Firewall-Schutz ausgenommen. Sie sollten den Schutz allerdings nur in begründeten Einzelfällen abschalten.



Wenn Sie ein Netzwerk mit der Maus markieren und den **Bearbeiten**-Button anklicken, können Sie die Firewall-Einstellungen für dieses Netzwerk einsehen bzw. verändern.

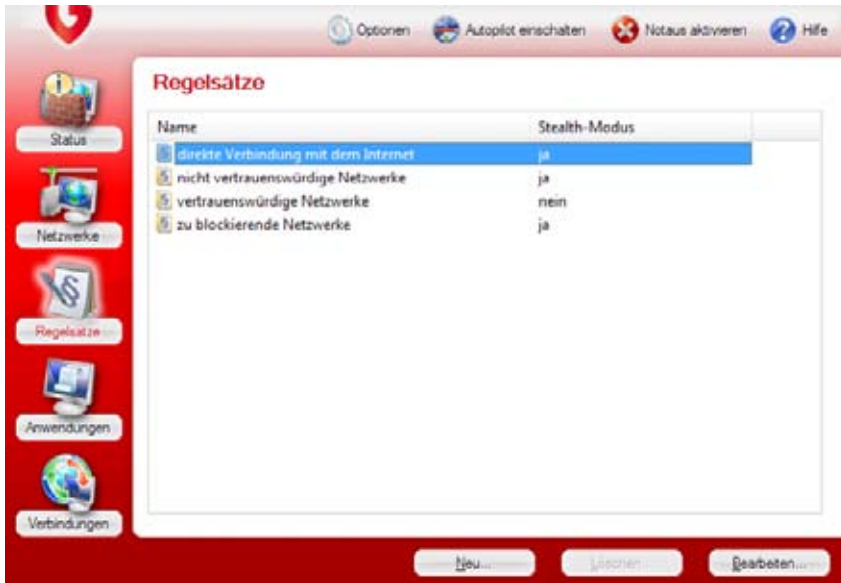
- **Netzwerk-Info:** Hier erhalten Sie Informationen zum Netzwerk, als - soweit vorhanden - Angaben zu **IP-Adresse, Subnetzmaske, Standardgateway, DNS- und WINS-Server.**
- **Firewall aktiv, auf diesem Netzwerk:** Sie können die Firewall für das Netzwerk hier deaktivieren, sollten dies allerdings nur in begründeten Einzelfällen tun.
- **Gemeinsame Nutzung der Internet-Verbindung:** Bei direkten Verbindungen mit dem Internet können Sie festlegen, ob alle über ein **TCP/IP-Netzwerk** verbundenen Rechner Zugriff aufs Internet haben sollen oder nicht. Diese **Interne tverbindungsfreigabe** (ICS) kann für ein Heimnetzwerk in der Regel aktiviert werden.
- **Automatische Konfiguration (DHCP) zulassen:** Bei der Verbindung Ihres Computers mit dem Netzwerk wird eine **dynamische IP-Adresse** (über das Dynamic Host Configuration Protocol) vergeben. Wenn Sie über diese Standardkonfiguration mit dem Netzwerk verbunden sind, sollten Sie das Häkchen hier gesetzt lassen.
- **Regelsatz:** Sie können hier sehr schnell zwischen vorstrukturierten Regelsätzen wählen und auf diese Weise festlegen, ob es sich bezüglich der Überwachungskriterien der Firewall z.B. um ein vertrauenswürdigen, nicht vertrauenswürdigen oder zu blockierendes Netzwerk handelt. Mit dem Button „**Regelsatz bearbeiten**“ haben Sie auch die Möglichkeit, die Regelsätze individuell zu konfigurieren. Lesen Sie hierzu bitte auch das Kapitel „**Regelsätze-Bereich**“.

■ Regelsätze-Bereich

Im **Regelsätze-Bereich** können Sie für verschiedene Netzwerke spezielle Regeln erstellen. Diese Regeln werden dann jeweils zu einem Regelsatz zusammengefasst. Voreingestellt sind Regelsätze für **direkte Verbindung mit dem Internet, nicht vertrauenswürdige Netzwerke, vertrauenswürdige Netzwerke** und **zu blockierende Netzwerke**.

In der Übersicht wird der jeweilige Regelsatz mit Namen und Stealth-Modus-Status angezeigt.

■ *Mit dem Stealth-Modus (engl.: verborgen, heimlich) werden Anfragen an den Computer, die dazu dienen, die Erreichbarkeit der jeweiligen Ports zu überprüfen nicht beantwortet. Dies erschwert Hackern, auf diese Weise Informationen über das System zu erhalten.*



Mit Hilfe der Buttons „**Neu**“, „**Löschen**“ und „**Bearbeiten**“ können Sie bestehende Regelsätze verändern, bzw. weitere Regelsätze hinzufügen.

■ Die drei vorgegebenen Regelsätze für direkte Verbindung mit dem Internet, vertrauenswürdige Netzwerke, nicht vertrauenswürdige Netzwerke und zu blockierende Netzwerke können nicht gelöscht werden. Regelsätze, die Sie selber erstellt haben, können Sie natürlich jederzeit löschen.

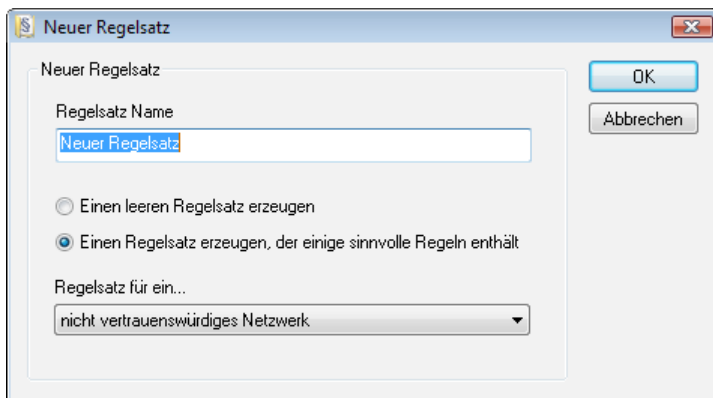
■ Regelsätze erstellen

Sie können jedem Netzwerk einen eigenen Regelsatz (also eine Sammlung speziell darauf abgestimmter Regeln) zuweisen. Auf diese Weise können Sie Netzwerke mit unterschiedlichen Gefährdungstufen unterschiedlich mit der Firewall absichern. So benötigt ein privates Heimnetzwerk sicherlich weniger Schutz (und damit auch Administrationsaufwand), als ein DFÜ-Netzwerk, das im direkten Kontakt mit dem Internet steht. Die Firewall beinhaltet drei voreingestellte Regelsätze für folgende Netzwerktypen:

- **Regelsatz für nicht vertrauenswürdige Netzwerke:** Hierunter fallen in der Regel offene Netzwerke, wie z.B. DFÜ-Netzwerke, die auf das Internet Zugriff haben.
- **Regelsatz für vertrauenswürdige Netzwerke:** Vertrauenswürdig sind in der Regel Heim- und Firmennetzwerke.

- **Regelsatz für zu blockierende Netzwerke:** Wenn zeitweise oder dauerhaft der Kontakt des Rechners zu einem Netzwerk blockiert werden soll, kann diese Einstellung verwendet werden. Dies macht z.B. Sinn bei der Verbindung mit fremden Netzwerken, über deren Sicherheitsstandard man sich nicht ganz im Klaren ist (z.B. auf LAN-Partys, fremden Firmennetzwerken, öffentlichen Arbeitsplätzen für Notebooks etc.)

Sie können neu etablierten Netzwerken auf Ihrem Computer einen entsprechend ausgewählten Regelsatz zuordnen. Darüber hinaus können Sie über den **Neu-**Button auch eigene Regelsätze für Netzwerke erstellen.

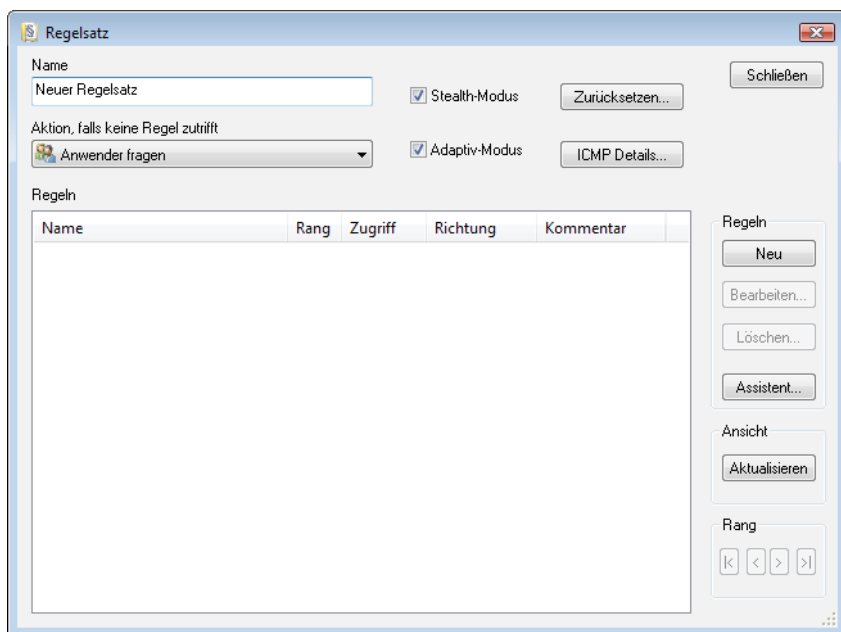
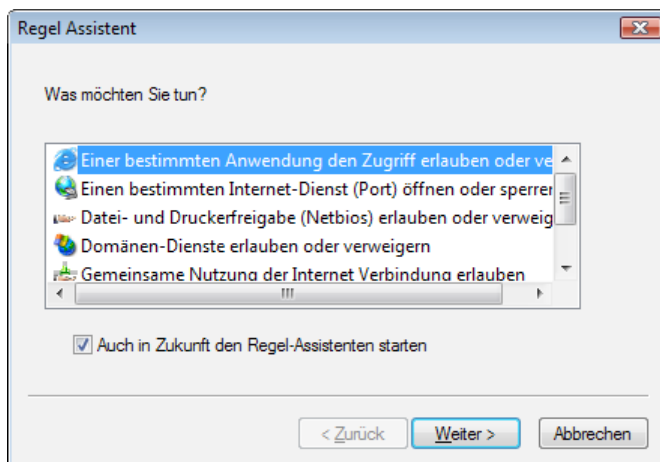


Klicken Sie dazu im Regelsätze-Bereich auf den **Neu**-Button und legen in dem erscheinenden Dialogfenster folgendes fest:

- **Regelsatzname:** Geben Sie hier einen aussagekräftigen Namen für den Regelsatz ein.
- **Einen leeren Regelsatz erzeugen:** Hier können Sie einen vollkommen leeren Regelsatz erzeugen und diesen ausschließlich mit selbstdefinierten Regeln bestücken.
- **Einen Regelsatz erzeugen, der einige sinnvolle Regeln enthält:** Bei dieser Auswahl können Sie entscheiden, ob beim neuen Regelsatz grundlegende Regeln für nichtvertrauenswürdige, vertrauenswürdige oder zu blockierende Netzwerke vordefiniert werden sollen. Auf Basis dieser Voreinstellungen können Sie dann individuelle Änderungen vornehmen.

Der neue Regelsatz erscheint nun im Regelsätze-Bereich unter dem jeweiligen Regelsatznamen (z.B. „**Neuer Regelsatz**“) in der Liste. Wenn Sie nun auf „**Bearbeiten**“ klicken, öffnet sich - je nach Einstellung, die Sie unter „**Optionen** >

Regelsätze“ (siehe gleichnamiges Kapitel) getroffen haben - der **Regel-Assistent** oder der **Profi-Dialog** zum Bearbeiten der einzelnen Regeln dieses Regelsatzes.



Wie Sie in den Regelsätzen neue Regeln vergeben, lesen Sie in den Kapiteln **„Regeln erstellen > Regel-Assistent verwenden“** bzw. **„Regeln erstellen > Profi-Dialog verwenden“**.

■ Neben der direkten Eingabe von Regeln haben Sie natürlich noch die Möglichkeit über die Info-Box des Firewall-Alarms Regeln zu erstellen. Dieser Lernprozess der Firewall wird Ihnen im Kapitel „Regeln erstellen > Firewall-Alarm“ erläutert.

■ Anwendungen-Bereich

Im Anwendungen-Bereich werden alle Programme aufgelistet, die aufs Netzwerk zugreifen.



Darüber hinaus liefert die Tabelle folgende Informationen:

- **Anwendung:** Der Dateiname der Anwendung, die mit dem Netzwerk in Verbindung tritt.
- **Zugriff:** Eine Information darüber, ob für die jeweilige Anwendung der Zugriff aufs Internet erlaubt oder verboten ist.
- **Protokoll:** Hier wird das verwendete Netzwerkprotokoll angezeigt
- **Netzwerk:** Die Art der Netzwerkanbindung wird hier spezifiziert.
- **Lokaler Port:** Angabe des lokalen Ports
- **Entfernte Adresse:** Die Zieladresse für den Netzwerkzugriff
- **Entfernter Port:** Der Zielport für den Netzwerkzugriff
- **Status:** Der Status der Netzwerkverbindung, ob es sich um eine verbundene (established), eine passive (listening) oder eine blockierte (blocked) Verbindung handelt.
- **Zeitmarke:** Datum des letzten Zugriffs aufs Netzwerk

Wenn Sie das Häkchen bei „**Systemanwendungen anzeigen**“ entfernen, werden die Systemanwendungen ausgeblendet und Sie sehen die Programme aufgelistet, die direkt mit dem Netzwerk in Verbindung treten. Über den Button „**Verbindungsdetails**“ können Sie sich zu ausgewählten Verbindungen einen detaillierten Überblick über die letzten Aktionen des Netzwerkzugriffs anzeigen lassen.

■ Ein Doppelklick auf den jeweiligen Eintrag unter „**Letzte Aktion**“ ermöglicht Ihnen einen Einblick in weitergehende Verbindungsdetails.

■ Verbindungen-Bereich

Im **Verbindungen-Bereich** werden alle von der Firewall erlaubten und blockierten Verbindungen mit Netzwerk und Internet protokolliert. Sie können diese Liste durch Anklicken der jeweiligen Spaltenüberschriften beliebig sortieren und mit Anklicken des **Details**-Button zu einzelnen Verbindungen weitergehende Informationen erhalten.

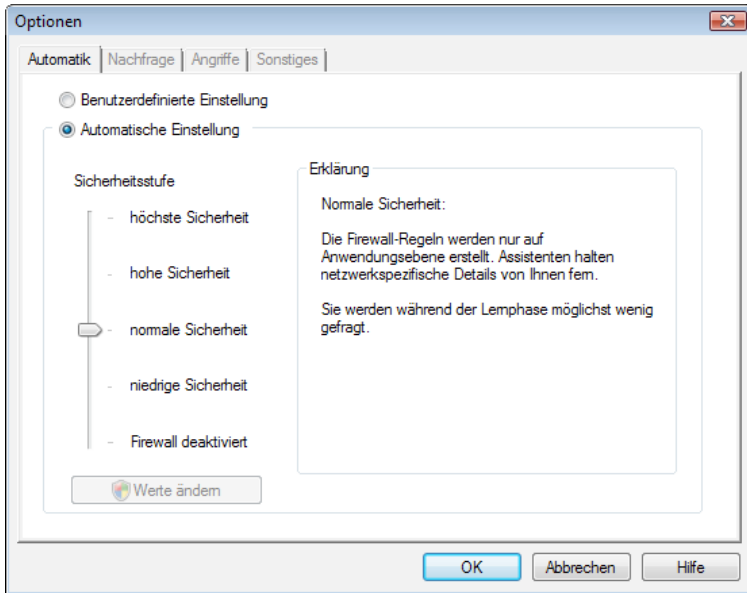


■ Optionen

Im **Optionen-Bereich** können Sie grundlegende Einstellungen der Software verändern. Klicken Sie dazu einfach die Registerkarte mit den jeweiligen Einstellungsoptionen an.

■ Automatik

Der Vorteil bei der Nutzung der vordefinierten Sicherheitsstufen liegt darin, ohne administrativen Aufwand und Fachkenntnisse im Bereich der Netzwerksicherheit die Firewall trotzdem auf individuelle Bedürfnisse anpassen zu können.



Stellen Sie einfach mit dem Schieberegler die **Sicherheitsstufe** ein, die Sie benötigen. Folgende Sicherheitsstufen stehen dabei zur Auswahl:

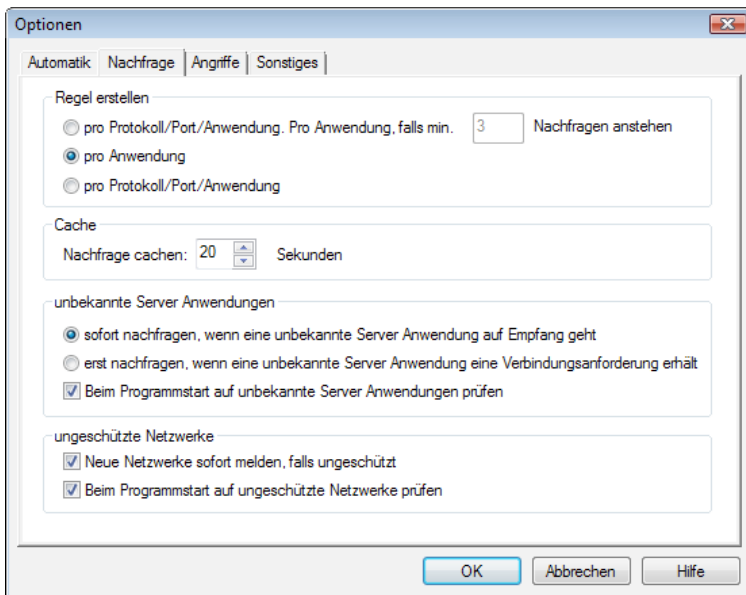
- **Höchste Sicherheit:** Die Firewall-Regeln werden mit sehr feinkörnigen Richtlinien erstellt. Dazu sollten Sie sich mit netzwerkspezifischen Fachbegriffen auskennen (TCP, UDP, Ports etc.). Die Firewall bemerkt kleinste Ungereimtheiten und wird während der Lernphase sehr häufig nachfragen.
- **Hohe Sicherheit:** Die Firewall-Regeln werden mit sehr feinkörnigen Richtlinien erstellt. Dazu sollten Sie sich mit netzwerkspezifischen Fachbegriffen auskennen (TCP, UDP, Ports etc.). Die Firewall wird während der Lernphase unter Umständen häufig nachfragen.
- **Normale Sicherheit:** Die Firewall-Regeln werden nur auf Anwendungsebene erstellt. Assistenten halten netzwerkspezifische Details von Ihnen fern. Sie werden während der Lernphase möglichst wenig gefragt.
- **Niedrige Sicherheit:** Die Firewall-Regeln werden nur auf Anwendungsebene erstellt. Assistenten halten netzwerkspezifische Details von Ihnen fern und Sie werden während der Lernphase selten gefragt. Höchst sicherer Schutz vor ankommenden Verbindungsanforderungen besteht auch in dieser Sicherheitsstufe.

- **Firewall deaktiviert:** Sie können die Firewall bei Bedarf auch abschalten. Ihr Computer ist dann weiterhin mit dem Internet und anderen Netzwerken verbunden, wird von der Firewall aber nicht mehr vor Angriffen oder Spionage-Attacken geschützt.

■ Wenn Sie die Firewall spezifischer einstellen möchten, setzen Sie bitte das Häkchen bei „benutzerdefinierte Einstellungen“. Beachten Sie aber, dass für diese Einstellungen zumindest ein Grundwissen zum Thema Netzwerksicherheit nötig ist.

■ Nachfrage

Hier legen Sie fest, wann, wie und ob die Firewall beim Anwender nachfragen soll, sobald Programme einen Verbindungsaufbau mit dem Internet oder Netzwerk anfragen.



Folgende Einstellungen sind dabei im Einzelnen möglich:

■ Regel erstellen

Wenn die Firewall eine Verbindungsaufnahme mit dem Netzwerk feststellt, erscheint eine Infobox, in der Sie festlegen, wie mit der jeweiligen Anwendung weiter zu verfahren ist. Hier können Sie festlegen, was genau Sie mit dem Erlauben oder Verbieten eines Netzwerkzugriffs bestimmen möchten:

- **pro Protokoll/Port/Anwendung. Pro Anwendung, falls min. ___ Nachfragen anstehen:** Es gibt Anwendungen (z.B. Microsoft Outlook), die bei einer Netzwerkanfrage gleich mehrere Ports anfragen bzw. gleichzeitig unterschiedliche Protokolle nutzen. Da dieses z.B. in der Einstellung „**pro Protokoll/Port/Anwendung**“ mehrere Abfragen über Info-Boxen mit sich brächte, kann hier auch festgelegt werden, dass Anwendungen eine generelle Freigabe bzw. Absage für die Netzwerknutzung erhalten, sobald Ihnen die Verbindung vom Anwender erlaubt oder untersagt wird.
- **pro Anwendung:** Hier wird der Netzwerkzugriff für die aktuell angezeigte Anwendung generell auf jedem Port und mit jedem Übertragungsprotokoll (z.B. TCP oder UDP) erlaubt oder verweigert.
- **pro Protokoll/Port/Anwendung:** Der Anwendung, die einen Netzwerkzugriff erfragt, erhält die Erlaubnis nur mit dem erfragten Übertragungsprotokoll und ausschließlich mit dem angefragten Port online zu gehen. Sollte dieselbe Anwendung einen weiteren Netzwerkzugriff auf einem anderen Port oder mit einem anderen Protokoll erfragen, erscheint die Info-Box erneut und es kann eine weitere Regel diesbezüglich erstellt werden.

■ Cache

Sie können erneut wiederkehrende **Verbindungsanfragen** einer Anwendung bündeln. Auf diese Weise erscheint bei Verbindungsversuchen, die sie noch nicht über eine Regel spezifiziert haben, nicht ständig eine Infobox, sondern z.B. nur in 20-Sekunden-Abständen oder einem anderen von Ihnen definierbaren Zeitraum.

■ Unbekannte Serveranwendungen

Anwendungen, die noch nicht über eine Regel in der Firewall verwaltet werden, können unterschiedlich behandelt werden. Der Zeitpunkt der Nachfrage steht dabei in einem gewissen Ermessensspielraum. Wenn die Serveranwendung „**auf Empfang**“ geht, heißt das, dass sie quasi auf Standby eine Verbindungsanforderung erwartet. Bei der Einstellung „**Verbindungsanforderung**“ erfolgt eben diese Verbindungsanforderung.

☐ *Generell sollten Sie das Häkchen bei „Beim Programmstart auf unbekannte Serveranwendungen prüfen“ gesetzt lassen, da sonst z.B. Trojaner, die vor dem Starten der Firewall auf dem Rechner waren, weiterhin aktiv bleiben können, ohne entdeckt zu werden.*

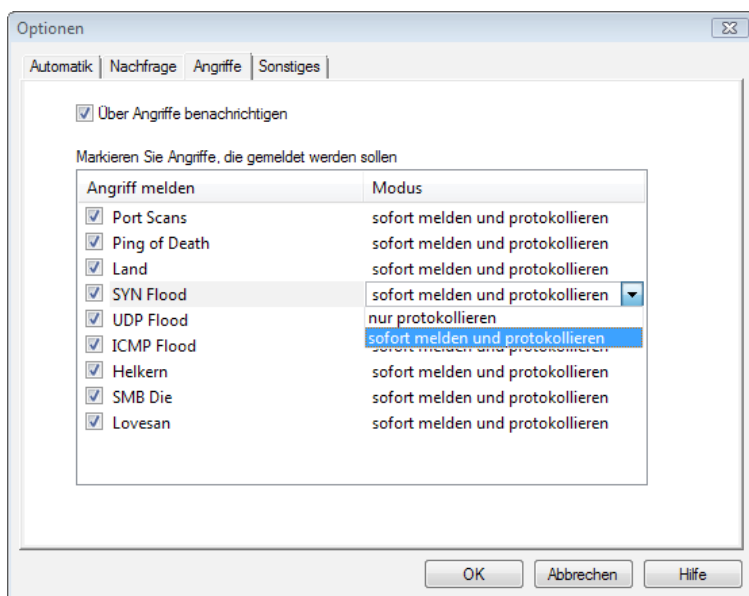
■ Ungeschützte Netzwerke

Natürlich kann eine Firewall nur dann problemlos funktionieren, wenn alle Netzwerke, auf die der zu schützende Rechner zugreift, von ihr auch erkannt und

überwacht werden. Sie sollten deshalb die Häkchen bei „**Neue Netzwerke sofort melden, falls ungeschützt**“ und „**Beim Programmstart auf ungeschützte Netzwerke prüfen**“ gesetzt lassen.

■ Angriffe

Generell sollten Sie die Häkchen für das Erkennen der unterschiedlichsten Hacker-Angriffe gesetzt lassen. Der geringe Performance-Vorteil, der sich dadurch ergibt, dass die Firewall diese Möglichkeiten der Einflussnahme nicht überprüft, steht in keinem Verhältnis zum Schaden, der durch einen geglückten Angriff entstehen kann.



Folgende Angriffsarten werden von der Firewall erkannt:

- **Port Scans:** Dabei werden die offenen TCP- und UDP-Ports auf einem angegriffenen Computer ermittelt. Ein solcher Angriff dient der Suche nach Schwachstellen im Computersystem und geht meist gefährlicheren Angriffen voraus.
- **Ping of Death:** Bei diesem Angriff wird ein ICMP-Paket gesendet, dessen Größe den zulässigen Wert von 64 KB überschreitet. Der Angriff kann zum Absturz bestimmter Betriebssysteme führen.
- **Land:** Bei diesem Angriff wird an einen offenen Port des angegriffenen Computers eine Anfrage auf Verbindungsherstellung mit sich selbst gesendet. Dies führt zu einer Endlosschleife im angegriffenen Computer, was eine stark

erhöhte Prozessorbelastung zur Folge hat und zum Absturz des Betriebssystems führen kann.

- **SYN Flood:** Bei diesem Angriff werden große Mengen falscher Verbindungsanfragen an den angegriffenen Computer gesendet. Das System reserviert für jede dieser Verbindungen bestimmte Ressourcen, wodurch es seine gesamten Ressourcen verbraucht und nicht auf Verbindungsanfragen anderer Quellen reagiert.
- **UDP Flood:** Bei diesem Angriff wird ein UDP-Paket gesendet, das auf Grund seiner Struktur endlos zwischen dem angegriffenen Computer und einer dem angegriffenen Computer frei zugänglichen Adresse hin- und hergeschickt wird. Dies führt auf beiden Computern zum Verlust von Ressourcen und erhöht die Belastung des Verbindungskanals.
- **ICMP Flood:** Bei diesem Angriff werden große Mengen von ICMP-Paketen an den angegriffenen Computer gesendet. Dies führt zu einer stark erhöhten Prozessorbelastung, da der Computer auf jedes Paket reagiert.
- **Helkern:** Bei diesem Angriff werden spezielle UDP-Pakete mit ausführbarem schädlichem Code an den angegriffenen Computer gesendet. Der Angriff führt zur Verlangsamung der Internetfunktionen.
- **Smb Die:** Bei diesem Angriff wird versucht, eine Verbindung nach SMB-Protokoll aufzubauen; bei erfolgreicher Verbindung wird an den angegriffenen Computer ein spezielles Paket gesendet, das versucht, den Puffer zu überfüllen. Als Folge wird der Computer neu gestartet. Dieser Angriff gefährdet die Betriebssysteme Windows 2k/XP/NT.
- **Lovesan:** Bei einem Angriff durch Lovesan wird versucht, auf Ihrem Computer Sicherheitslücken im Service DCOM RPC der Betriebssysteme Windows NT 4.0/NT 4.0 Terminal Services Edition/2000/XP/Server(tm) 2003 zu ermitteln. Sind solche Schwachstellen auf dem Computer vorhanden, dann wird ein Programm mit schädlichen Funktionen gesendet, das es erlaubt, auf Ihrem Computer beliebige Manipulationen vorzunehmen.

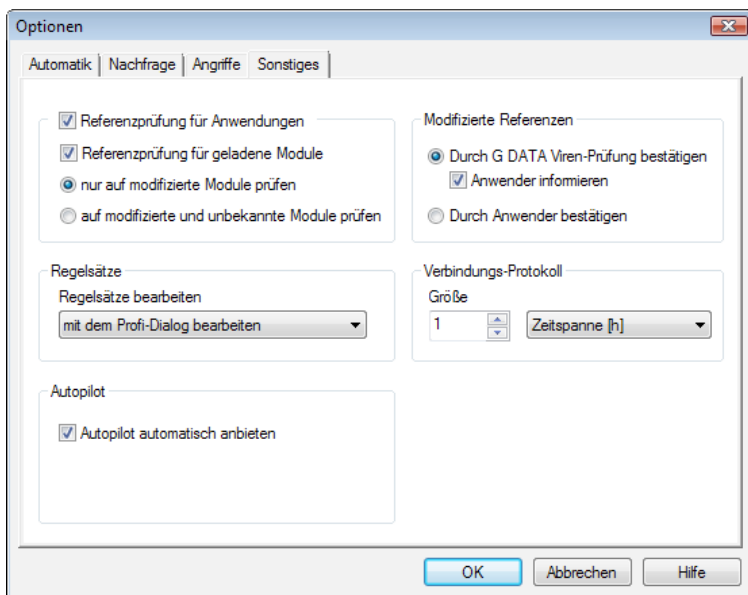
■ Wenn Sie die Angaben in der Spalte „Modus“ anklicken, können Sie festlegen, ob Hacker-Angriffe per Dialogbox sofort gemeldet oder nur protokolliert werden sollen.

■ Sonstiges

■ Referenzprüfung

Bei der Referenzprüfung wird für Anwendungen, denen von der Firewall schon der Zugriff aufs Netzwerk erlaubt wurde, eine **Prüfsumme** auf Basis der Dateigröße und anderer Kriterien ermittelt. Wenn diese Prüfsumme des Programms plötzlich abweicht, kann es daran liegen, dass das Programm durch ein Schadprogramm

verändert wurde. In diesem Fall schlägt die Firewall Alarm. Die **Referenzprüfung für Anwendungen** sollte in der Regel eingeschaltet bleiben.



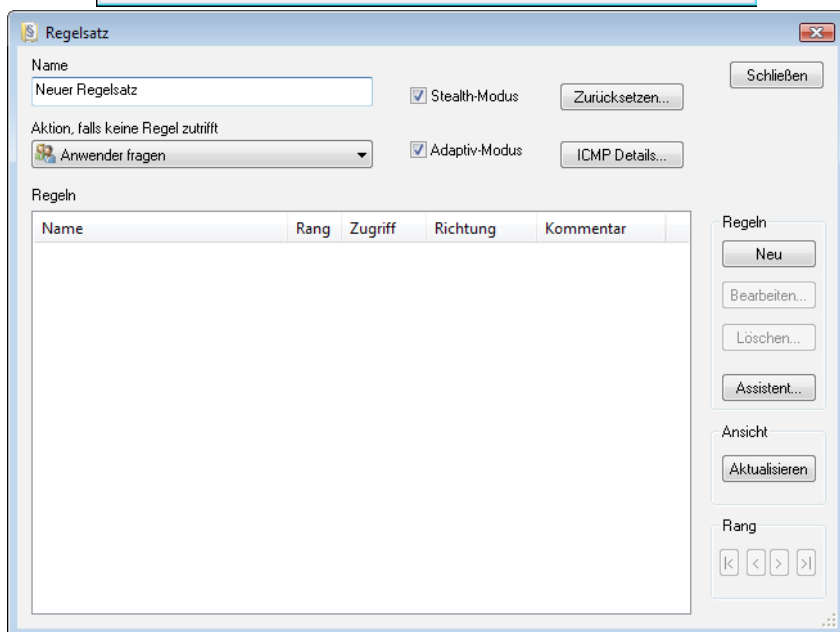
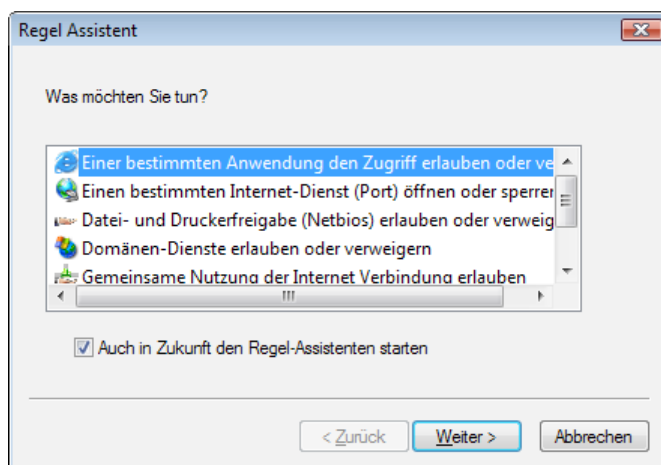
Die **Referenzprüfung für geladene Module** beobachtet auf gleiche Weise die **Module**, die die Anwendungen verwenden (z.B. **DLLs**). Da diese sich häufig ändern oder auch neue Module nachgeladen werden, kann eine konsequente Prüfung auf modifizierte **und** unbekannte Referenzen bei Modulen zu einem erheblichen Administrationsaufwand bei der Nutzung der Firewall führen. Jedes geänderte Modul würde dann nämlich eine Sicherheitsabfrage der Firewall nach sich ziehen. Die Modulprüfung sollte deshalb nur bei sehr hohen Ansprüchen an die Sicherheit in dieser Weise genutzt werden.

Die **Referenzprüfung für modifizierte Referenzen** (z.B. bei einem Windows-Update) kann weitestgehend automatisiert werden, wenn die Module über das G DATA Antiviren-Modul geprüft und für unbedenklich gefunden wurden. Sollten das Antiviren-Modul nicht installiert sein, kann die Bestätigung für modifizierte Referenzen auch manuell durch den Anwender erfolgen.

■ Regelsätze

Hier können Sie festlegen, ob Sie das Erstellen neuer Regeln über den **Regel-Assistenten** oder mit dem **Profi-Dialog** durchführen möchten. Für Anwender, die sich in der Materie der Netzwerksicherheit nicht auskennen, empfehlen wir den Regel-Assistenten.

■ Natürlich kann man vom Regel-Assistenten auch jederzeit direkt zum Profi-Dialog wechseln und auch ein Wechsel in die andere Richtung ist jederzeit möglich. Wählen Sie dazu beim Regel-Assistenten einfach unter „Was möchten Sie tun?“ den Eintrag „In den erweiterten Bearbeitungsmodus wechseln“ aus oder klicken Sie im Profi-Dialog auf den Assistent-Button.



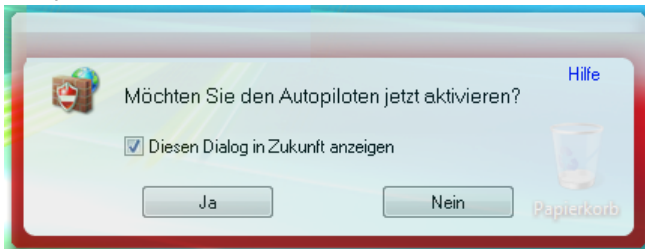
■ Verbindungs-Protokoll

Hier können Sie festlegen, wie lange die Firewall **Verbindungsdaten aufbewahren** soll. Sie können die Daten von einer Stunde bis zu 56 Stunden nachhalten und im Programmbereich „**Verbindungen**“ einsehen. Lesen Sie hierzu auch das Kapitel „**Verbindungen-Bereich**“.

■ Autopilot

Beim Computer-Spielen (und anderen Full-Screen Anwendungen) kann es störend sein, wenn die Firewall mit vielen Nachfragen den Spielfluss oder einfach nur die Darstellung stört. Um einen ungestörten Spielgenuss ohne Sicherheitseinbußen zu gewährleisten gibt es den „**Autopiloten**“. Wenn dieser aktiviert ist, werden direkt bei der ersten Anfrage (z.B. für eine Online-Verbindung) alle Programmteile und Komponenten des Spieles gescannt und ihnen bei Unbedenklichkeit ein Zugriff aufs Netzwerk gestattet. Diese Nachfrage bündelt also Einzelnachfragen und vereinfacht so den Firewallschutz für diese speziellen Anwendungen.

- *Wenn die Firewall erkennt, dass eine Fullscreen-Anwendung gestartet wird und der Autopilot ist nicht aktiv, wird von der Software vorgeschlagen, den Autopiloten zu aktivieren.*



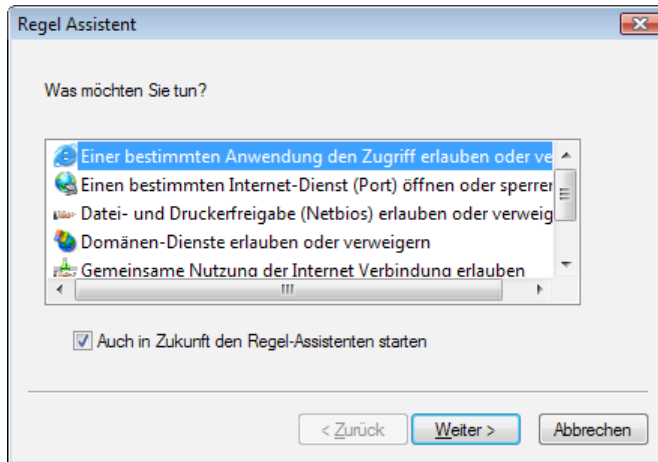
■ Regeln erstellen

■ Regel-Assistenten verwenden

Mit dem **Regel-Assistenten** können Sie bestimmte zusätzliche Regeln für den jeweiligen Regelsatz definieren oder bestehende Regeln ändern. Gerade für Anwender, die sich nicht gut mit der Firewalltechnologie auskennen, ist der Regel-Assistent dem Profi-Dialog vorzuziehen.

- *Mit dem Regel-Assistenten verändern Sie eine oder mehrere Regeln in dem jeweils ausgewählten Regelsatz. Sie erstellen also immer eine Regel innerhalb eines Regelsatzes, der verschiedene Regeln beinhaltet.*

- *Abhängig davon, welchen Regelsatz Sie für das jeweilige Netzwerk definiert haben, kann eine Anwendung in dem einen Regelsatz (z.B. für nicht vertrauenswürdige Netze) gesperrt sein, in dem anderen Regelsatz (z.B. für vertrauenswürdige Netze) vollen Netzzugriff haben. So könnten Sie z.B. einen Browser mit entsprechend unterschiedlichen Regeln so beschränken, dass er wohl auf Seiten zugreifen kann, die in ihrem Heimnetzwerk bereitstehen, aber keine Möglichkeit hat, auf Inhalte aus dem DFÜ-Netzwerk zuzugreifen.*



Der Regel-Assistent stellt Ihnen folgende Basisregeln zur Verfügung:

- **Einer bestimmten Anwendung den Zugriff erlauben oder verweigern:** Hiermit können Sie gezielt eine Anwendung (ein Programm) auf Ihrer Festplatte auswählen und ihm explizit den Zugriff auf das über den Regelsatz definierte Netzwerk erlauben oder verbieten. Wählen Sie im Assistenten dazu einfach das gewünschte Programm aus (Programmpfad) und geben Sie dann unter „**Verbindungsrichtung**“ an, ob das Programm für eingehende Verbindungen, ausgehende Verbindungen oder sowohl ein-, als auch ausgehende Verbindungen gesperrt werden soll. Auf diese Weise können Sie z.B. ihre MP3-Playersoftware ggf. daran hindern, Daten über Ihre Hörgewohnheiten weiterzugeben (ausgehende Verbindung) oder dafür sorgen, dass nicht automatisch Programmupdates aufgespielt werden (eingehende Verbindung).
- **Einen bestimmten Internet-Dienst (Port) öffnen oder sperren:** Als **Port** werden spezielle Adressbereiche bezeichnet, die über ein Netzwerk übermittelte Daten automatisch an ein bestimmtes **Protokoll** und darüber an bestimmte Software weiterleiten. So wird z.B. die Übermittlung von regulären Websites über den Port „80“ abgewickelt, E-Mail-Versand über den Port „25“, E-Mail-Abholung

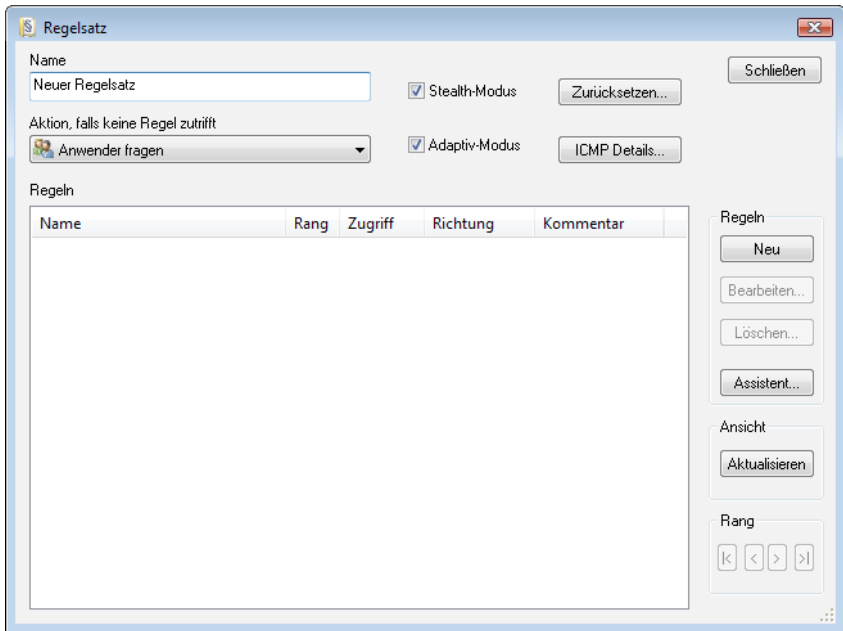
über Port „110“ usw. Ohne Firewall stehen an Ihrem Computer generell alle Ports offen, obwohl die meisten von normalen Anwendern gar nicht benötigt werden. Über das Sperren eines oder mehrerer Ports können deshalb schnell Lücken geschlossen werden, die sonst von Hackern für Angriffe genutzt werden könnten. Im Assistenten haben Sie die Möglichkeit Ports komplett zu sperren oder aber auch nur für eine bestimmte Anwendung (z.B. Ihre MP3-Abspielsoftware).

- **Datei- und Druckerfreigabe (Netbios) erlauben oder verweigern:** Das **NetBIOS** ist eine spezielle Schnittstelle in Netzwerken und kann dazu genutzt werden z.B. Datei- oder Druckerfreigaben direkt von Rechner zu Rechner durchzuführen, ohne dabei z.B. das TCP/IP-Protokoll zu nutzen. Da dies in Heimnetzwerken meistens unnötig ist und das NetBIOS von Hackern dazu genutzt werden kann, einen Rechner lahmzulegen, ist es in vielen Fällen ratsam, diese Freigabe für nicht vertrauenswürdige Netze zu verweigern.
- **Domänen-Dienste erlauben oder verweigern:** Eine **Domäne** ist eine Art Gliederungsverzeichnis für Computer in einem Netzwerk und ermöglicht damit eine zentralisierte Verwaltung der im Netzwerk eingebunden Rechner. Freigaben für Domänen-Dienste in nicht vertrauenswürdigen Netzen sollten in der Regel verweigert werden.
- **Gemeinsame Nutzung der Internet-Verbindung erlauben:** Bei direkten Verbindungen mit dem Internet können Sie festlegen, ob alle über ein **TCP/IP-Netzwerk** verbundenen Rechner Zugriff aufs Internet haben sollen oder nicht. Diese **Internetverbindungsfreigabe** (ICS) kann für ein Heimnetzwerk in der Regel aktiviert werden.
- **In den erweiterten Bearbeitungsmodus (Profi-Dialog) wechseln:** Hiermit können Sie vom Regel-Assistenten zum Profi-Dialog wechseln. Informationen zum Profi-Dialog erhalten Sie im Kapitel „**Regeln erstellen > Profi-Dialog verwenden**“.

■ Wenn Sie das Häkchen bei „Auch in Zukunft den Regel-Assistenten starten“ entfernen, öffnet die Firewall für neue Regeln automatisch den Profi-Dialog.

■ Profi-Dialog verwenden

Im Profi-Dialog können Sie - gewisse Kenntnisse in Netzwerksicherheit vorausgesetzt - sehr individuelle Regeln für das jeweilige Netzwerk definieren. Dabei können natürlich sämtliche Regeln erzeugt werden, die Sie auch über den **Regel-Assistenten** erzeugen können, aber auch darüber hinaus weitergehende Einstellungen vorgenommen werden.



Folgende Einstellungsmöglichkeiten stehen Ihnen hier zur Verfügung:

■ Name

Hier können Sie den Namen für den aktuellen Regelsatz gegebenenfalls verändern. Unter diesem Namen wird der Regelsatz dann in der Liste im Regelsätze-Bereich angezeigt und kann mit den dort von der Firewall identifizierten Netzwerken kombiniert werden.

■ Stealth-Modus

Mit dem Stealth-Modus (engl.: verborgen, heimlich) werden Anfragen an den Computer, die dazu dienen, die Erreichbarkeit der jeweiligen Ports zu überprüfen nicht beantwortet. Dies erschwert Hackern, auf diese Weise Informationen über das System zu erhalten.

■ Aktion, falls keine Regel zutrifft

Hier können Sie festlegen, ob der Zugriff im Netzwerk generell erlaubt, verweigert oder auf Nachfrage geregelt werden soll. Sollten durch die Lernfunktion der Firewall für einzelne Programme Sonderregeln definiert sein, werden diese natürlich berücksichtigt.

■ Adaptiv-Modus

Der Adaptiv-Modus unterstützt Sie bei Anwendungen, die die sogenannte „**Rückkanal-Technik**“ verwenden (z.B. **FTP** und viele **Online-Spiele**). Solche Anwendungen verbinden sich mit einem entfernten Rechner und handeln mit ihm einen Rückkanal aus auf dem sich der entfernte Rechner mit Ihrer Anwendung „zurückverbindet“. Ist der Adaptiv-Modus aktiv, so erkennt die Firewall diesen Rückkanal und lässt ihn zu ohne gesondert deshalb nachzufragen.

■ ICMP-Details

Das Internet Control Message Protocol (ICMP) ist ein Internet-Protokoll, welches in Netzwerken dazu genutzt wird Diagnose-Informationen für den Datentransfer zu übermitteln. Natürlich können ICMP-Informationen auch dazu genutzt werden, einen Rechner auszuspähen. Aus diesem Grund können die ICMP-Nachrichten über die Firewall unterdrückt werden. Um hier ohne Regel-Assistent Änderungen vorzunehmen, sollten Sie sich mit ICMP auskennen.

■ Regeln

In der Liste der Regeln finden Sie sämtliche Regeln, die als **Ausnahmetatbestände** für diesen Regelsatz definiert wurden. So können hier z.B. ausgewählten Programmen umfangreiche **Netzzugriffe** gestattet werden, obgleich das Netzwerk

an sich als nicht vertrauenswürdig definiert wird. Die Regeln, die hier einfließen, können auf verschiedene Weise erzeugt worden sein:

- Über den Regel-Assistenten
- Direkt über den Profi-Dialog über den **Neu**-Button
- Über den Dialog in der Info-Box, die bei einem Firewall-Alarm erscheint.

Jeder Regelsatz hat natürlich eine eigene Liste mit Regeln.

■ *Da die Firewall-Regeln teilweise hierarchisch verschachtelt sind, ist es in manchen Fällen wichtig, die Rangfolge bei den Regeln zu beachten. So kann es sein, dass eine Freigabe für einen Port durch die Verweigerung eines Protokollzugriffs wieder blockiert werden kann. Sie können den Rang einer Regel in der Abfolge ändern, indem Sie diese mit der Maus markieren und dann über die Pfeiltasten unter „Rang“ in der Liste hinauf- oder hinabbewegen.*

Regel bearbeiten - Regelsatz: Neuer Regelsatz

Name: ☒ Regel aktiv

Kommentar:

Verbindungs-Richtung: Zugriff:

☐ Protokoll:

☐ Zeitfenster: von bis

☐ IP-Adressraum: von bis

Wenn Sie eine neue Regel über den Profi-Dialog erstellen oder eine bestehende Regel über den Bearbeiten-Dialog verändern, erscheint der „**Regel bearbeiten**“ Dialog mit folgenden Einstellungsmöglichkeiten:

- **Name:** Hier findet sich bei voreingestellten und automatisch generierten Regeln der Programmname für den die jeweilige Regel zutrifft. Sie können den Namen

über den **Bearbeiten**-Button auch jederzeit verändern oder um zusätzliche Informationen ergänzen.

- **Regel aktiv:** Sie können eine Regel durch Entfernen des Häkchens inaktiv setzen, ohne sie gleich zu löschen.
- **Kommentar:** Hier erfahren Sie, auf welche Weise die Regel erzeugt wurde. Bei für den Regelsatz voreingestellten Regeln steht „**Voreingestellte Regel**“, bei Regeln, die sich aus dem Dialog aus dem Firewall-Alarm ergeben steht „**per Nachfrage generiert**“ und für Regeln, die Sie selber über den Profi-Dialog generieren, können Sie einen eigenen Kommentar einfügen.
- **Richtung / Verbindungsrichtung:** Mit der Richtung wird definiert, ob es sich bei dieser Regel um eine Regel für eingehende, ausgehende oder ein- und ausgehende Verbindungen handelt.
- **Zugriff:** Hier wird eingestellt, ob für das jeweilige Programm innerhalb dieses Regelsatzes der Zugriff erlaubt oder verweigert werden soll.
- **Protokoll:** Hier können Sie auswählen, welchen Verbindungsprotokollen Sie einen Zugriff erlauben oder verwehren wollen. Dabei haben Sie die Möglichkeit, Protokolle generell zu sperren oder freizugeben oder die Verwendung des Protokolls mit der Nutzung einer bestimmten Anwendung oder mehrerer Anwendungen zu koppeln („**Anwendungen zuordnen**“). Genauso können Sie die unerwünschten bzw. erwünschten Ports über den Button „**Internet-Dienst zuordnen**“ genau definieren.
- **Zeitfenster:** Sie können den Zugriff auf Netzwerkressourcen auch zeitabhängig gestalten und so z.B. dafür sorgen, dass ein Zugriff nur zu Ihren Arbeitszeiten und nicht außerhalb dieser Zeiten erfolgt.
- **IP-Adressraum:** Gerade für Netzwerke mit fest vergebenen IP-Adressen macht es Sinn, deren Nutzung über eine Beschränkung des IP-Adressraumes zu reglementieren. Ein klar definierter IP-Adressraum verringert die Gefahr eines Hackerangriffs deutlich.

■ Firewall-Alarm

Generell fragt die Firewall bei unbekannten Programmen und Prozessen, die mit dem Netzwerk in Verbindung treten wollen, nach, ob dies erlaubt oder verweigert werden soll. Dazu öffnet sich eine Info-Box, in der Ihnen Details zur jeweiligen Anwendung geliefert werden. Hier haben Sie auch die Möglichkeit, der Anwendung einen Zugriff auf das Netzwerk einmal oder auch dauerhaft zu erlauben oder zu verweigern. Sobald Sie einem Programm den Zugriff dauerhaft erlauben oder verweigern, wird dies als Regel in den Regelsatz des jeweiligen Netzwerkes aufgenommen und von nun an nicht mehr nachgefragt.



Hier stehen Ihnen folgende Button zur Verfügung:

- **Immer erlauben:** Über diesen Button erstellen Sie für die oben aufgeführte Anwendung (z.B. Opera.exe oder Explorer.exe oder iTunes.exe) eine Regel, die in dem genannten Netzwerk der Anwendung einen dauerhaften Zugriff aufs Netzwerk bzw. Internet erlaubt. Diese Regel finden Sie dann auch als „**auf Nachfrage erzeugte Regel**“ im Bereich „**Regelsätze**“.
- **Temporär erlauben:** Über diesen Button erlauben Sie der jeweiligen Anwendung nur ein einziges Mal Zugriff aufs Netzwerk. Beim nächsten Versuch eines Netzwerkzugriffs durch dieses Programm fragt die Firewall erneut nach.
- **Immer verweigern:** Über diesen Button erstellen Sie für die oben aufgeführte Anwendung (z.B. dialer.exe oder spam.exe oder trojan.exe) eine Regel, die in dem genannten Netzwerk der Anwendung einen dauerhaften Zugriff aufs Netzwerk bzw. Internet verweigert. Diese Regel finden Sie dann auch als „**auf Nachfrage erzeugte Regel**“ im Bereich „**Regelsätze**“.
- **Temporär verweigern:** Über diesen Button verbieten Sie der jeweiligen Anwendung nur ein einziges Mal den Zugriff aufs Netzwerk. Beim nächsten Versuch eines Netzwerkzugriffs durch dieses Programm fragt die Firewall erneut nach.

Darüber hinaus stehen Ihnen hier noch weitere Funktionen zur Verfügung:

■ Details

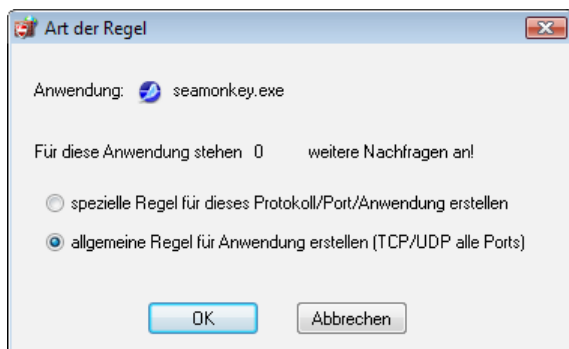
Wenn Sie auf den **Details**-Button klicken, erhalten Sie weitere Informationen zu Protokoll, Port und IP-Adresse mit der die jeweilige Anwendung interagieren möchte.



Wenn Sie den Button hinter „**Wollen sie das erlauben**“ anklicken, können Sie die unter „**Optionen > Nachfrage > Regel erstellen**“ voreingestellten Parameter für eine Regel individuell ändern:

- **spezielle Regel für dieses Protokoll/Port/Anwendung erstellen:** Der Anwendung, die einen Netzwerkzugriff erfragt, erhält die Erlaubnis nur mit dem erfragten Übertragungsprotokoll und ausschließlich mit dem angefragten Port online zu gehen. Sollte dieselbe Anwendung einen weiteren Netzwerkzugriff auf einem anderen Port oder mit einem anderen Protokoll erfragen, erscheint die Info-Box erneut und es kann eine weitere Regel diesbezüglich erstellt werden.
- **allgemeine Regel für Anwendung erstellen (TCP/UDP alle Ports):** Hier wird der Netzwerkzugriff für die aktuell angezeigte Anwendung generell auf jedem Port und mit jedem Übertragungsprotokoll (z.B. TCP oder UDP) erlaubt oder verweigert.

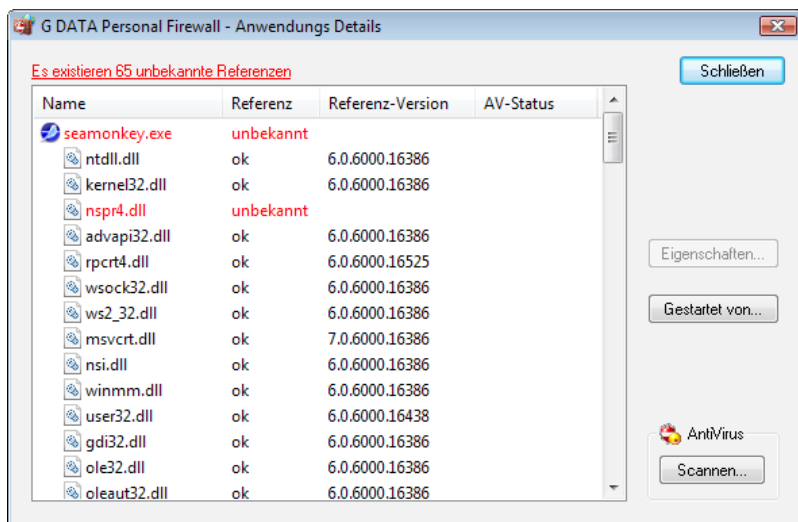
■ *In der Regel reichen bei normaler Nutzung der Firewall die allgemeinen Regeln durchaus aus.*



■ Anwendung auf Viren und Schadfunktionen überprüfen

Sie können den Namen der angezeigten Anwendung, sowie die Anwendung, die diese nutzt, um aufs Netzwerk zuzugreifen (z.B. den Internet Explorer "Explorer.EXE") anklicken, um diese speziell auf Viren und Schadfunktionen zu überprüfen. Diese Überprüfung kann Ihnen bei Programmen, deren Funktion Ihnen nicht auf Anhieb ersichtlich ist, bei der Entscheidung über eine Netzwerkfreigabe helfen. Klicken Sie dazu einfach im Fenster "**Anwendungsdetails**" auf den **Scannen**-Button unter dem Security-Symbol.

■ *Sollte AntiVirus nicht installiert sein, kann eine entsprechende Überprüfung natürlich nicht stattfinden.*



■ Paket-Info

Je nach Anwendung können Sie sich auch weitergehende Informationen zu geblockten oder übermittelten Datenpaketen anzeigen lassen. Hierbei handelt es sich aber um Informationen, die eher für Spezialisten interessant sind und für den allgemeinen Gebrauch der Firewall nicht notwendigerweise zu beachten sind.

■ Die Bedienung von AntiSpam

Sonderangebote, Werbungen, Newsletter – die Flut an unerwünschten E-Mails steigt immer weiter. Quillt Ihr Posteingang über dank Unmengen an unerwünschter elektronischer Post? AntiSpam schützt sicher vor Spam-Müll, blockiert Spam-Absender effizient und verhindert Fehlkennungen aufgrund der Kombination modernster Spam-Prüfungskriterien – damit Sie sich künftig über neue Mails wieder freuen können. Die **Bedienung von AntiSpam** ist prinzipiell selbsterläuternd und übersichtlich gestaltet. Anhand unterschiedlicher Karteikarten, die Sie über die links in AntiSpam angezeigten Symbole anwählen können, wechseln Sie in den jeweiligen Programmbereich und können dort Aktionen durchführen, Voreinstellungen vornehmen oder Vorgänge überprüfen.



Folgende Programmbereiche stehen Ihnen zur Verfügung

- **Mailstatus:** Im Status-Bereich von AntiSpam erhalten Sie grundlegende Informationen zum aktuellen Zustand Ihres Systems und von AntiSpam.
- **Weitere Filter:** Im Filter-Bereich können Sie auf komfortable Weise Filter nutzen, die eingehende Mails blocken oder automatisch möglicherweise gefährlichen Inhalte aus Mails entfernen.

- **Statistik:** Im Statistik-Bereich erhalten Sie eine ausführliche statistische Auswertung der Spam-relevanten Vorgänge auf Ihrem Mail-Server.
- **Kein Spam:** Hier erhalten Sie eine ausführliche Übersicht über alle Mails, die von AntiSpam nicht als Spam definiert wurden.
- **Spam:** Hier erhalten Sie eine ausführliche Übersicht über alle Mails, die von AntiSpam als Spam definiert wurden.

Außerdem finden Sie in der oberen Menüleiste der AntiSpam-Programmoberfläche übergreifende Funktionen und Einstellungsmöglichkeiten.



Optionen: Hier können Sie grundlegende Einstellungen zum Betrieb von AntiSpam verändern und an individuelle Bedürfnisse anpassen.



Spam-Filter: Hier können Sie umfangreiche Einstellungen vornehmen, um Ihren Mail-Server vor dem Empfang von Spam-Mails zu schützen. Über die Einstellung verschiedener Spam-Verdachtsstufen können Sie auch den Umgang mit Spam-ähnlichen Mails (z.B. Newslettern) für den Anwender übersichtlich gestalten und so die Zeit, die mit dem Sichten unnötiger Mails verbracht wird, effektiv reduzieren.



Hilfe-Bereich: Hier rufen Sie die Online-Hilfe zum Produkt auf.

■ Programmbereiche

■ Status

Im Status-Bereich von AntiSpam erhalten Sie grundlegende Informationen zum aktuellen Zustand Ihres Systems und von AntiSpam. Diese finden sich rechts vom jeweiligen Eintrag als Textangabe.



Ein grünes **Häkchen** weist darauf hin, dass die jeweilige Komponente aktiv ist und ihre Schutzfunktion erfüllt.



Ein rotes **Verbotsschild** informiert darüber, dass die entsprechende Komponente nicht aktiv ist und die jeweilige Schutzfunktion nicht zur Verfügung steht.

Durch doppeltes Anklicken des jeweiligen Eintrags (oder durch Auswählen des Eintrags und Anklicken des **Bearbeiten**-Buttons) können Sie hier direkt Aktionen vornehmen oder in den jeweiligen Programmbereich wechseln. Sobald Sie die

Einstellungen einer Komponente mit **Achtung-Symbol** optimiert haben, wechselt das Symbol im Status-Bereich wieder auf das grüne **Häkchensymbol**.



Folgende Einträge stehen Ihnen zur Verfügung

- **Spam-Filter:** Mit einem Doppelklick auf diesen Eintrag gelangen Sie in das dazugehörige Einstellungsfenster (Filter-Bereich: Spam filtern) und können dort umfangreiche Einstellungen vornehmen, um Ihr System vor dem Empfang von Spam-Mails zu schützen.
- **Spam-OutbreakShield:** Mit dem OutbreakShield können Schädlinge in Massenmails schon erkannt und bekämpft werden, bevor aktualisierte Virensignaturen dafür verfügbar sind. Das OutbreakShield erfragt dabei über das Internet besondere Häufungen von verdächtigen Mails und schließt dabei quasi in Echtzeit die Lücke, die zwischen dem Beginn eines Massenmailings und seiner Bekämpfung durch speziell angepasste Virensignaturen besteht.
- **HTML-Skripte deaktivieren:** Mit einem Doppelklick auf diesen Eintrag (Filter-Bereich: HTML-Skripte deaktivieren) können Sie HTML-Skripte deaktivieren. Skripte in HTML-formatierten Mails können im Gegensatz zu ‚gewöhnlichen‘ Dateianhängen ihre möglichen Schadroutine schon ausführen, wenn der Anwender die Mail in der Vorschauansicht seines Mailprogrammes aufruft. Insoweit ist gerade hier Vorsicht geboten.

- **Gefährliche Anhänge filtern:** Sie haben umfangreiche Funktionen, um gefährliche Dateianhänge zu entfernen, inaktiv zu schalten oder den Anwender vor ihnen zu warnen. Mit einem Doppelklick auf diesen Eintrag gelangen Sie in den Einstellungsbereich (Filter-Bereich: Anhänge filtern), in dem Sie entsprechende Filterregeln definieren können.

■ Weitere Filter

Im **Filter-Bereich** können Sie auf komfortable Weise Filter nutzen, die eingehende Mails blocken oder automatisch möglicherweise gefährlichen Inhalte aus Mails entfernen. Dazu können Sie über den **Neu**-Button im neue Filterregeln anlegen oder über den **Bearbeiten**-Button vorhandene Filter bearbeiten.

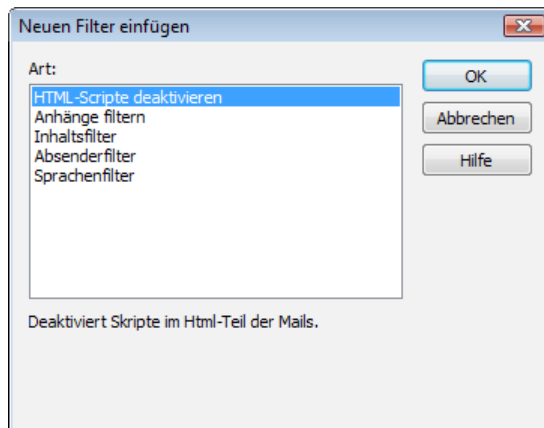


Die erstellten Filter werden in der Liste im Filter-Bereich angezeigt und können über die Häkchenfelder links vom jeweiligen Eintrag beliebig an- bzw. abgeschaltet werden. Wenn sich ein Häkchen im Häkchenfeld befindet, ist der jeweilige Filter aktiv. Wenn sich kein Häkchen im Häkchenfeld befindet, ist der Filter nicht aktiv. Um einen Filter endgültig zu löschen, markieren Sie diesen bitte mit einem einfachen Mausklick und verwenden dann den **Löschen**-Button.

■ Bei den Filtermöglichkeiten, die Ihnen im Bereich „Weitere Filter“ zur Verfügung stehen, handelt es sich um zusätzliche Filter, die den eigentlichen Spam-Filter von AntiSpam unterstützen und Ihnen individuelle Einstellungen erleichtern. Über

den eigentlichen Spam-Filter (- wie er im Kapitel „Spam-Filter“ erläutert wird -) haben Sie umfangreiche Einstellungsmöglichkeiten, um Mails mit unerwünschten Inhalten oder von unerwünschten Absendern (z.B. Massenmailversendern) wirkungsvoll zu blockieren. Das Programm prüft viele Merkmale der Mails, die typisch für Spam sind. Anhand der zutreffenden Merkmale wird ein Wert errechnet, der die Wahrscheinlichkeit für Spam widerspiegelt. Dazu stehen Ihnen mehrere Karteikarten zur Verfügung, in denen Ihnen alle relevanten Einstellungsmöglichkeiten thematisch gegliedert zur Verfügung stehen.

Wenn Sie einen neuen Filter anlegen, öffnet sich ein **Auswahlfenster**, in dem Sie den grundlegenden Filtertyp festlegen können. Alle weiteren Angaben zum zu erstellenden Filter können Sie dann in einem dem Filtertyp angepassten Assistentenfenster angeben. Auf diese Weise erstellen Sie auf sehr komfortable Weise Filter gegen jede erdenkliche Gefährdung.



Die unterschiedlichen Filtertypen werden in den folgenden Abschnitten ausführlich erläutert: Generell können Sie bei allen Filtertypen unter „**Name**“ einen aussagekräftigen Namen für den jeweiligen Filter angeben, mit dem dieser Filter dann in der Liste des Filter-Bereichs angezeigt wird und Sie können unter „**Bemerkung**“ interne Bemerkungen und Notizen zu dem betreffenden Filter angeben.

■ HTML-Skripte deaktivieren

Dieser Filter deaktiviert Skripte im HTML-Teil einer Mail. Skripte, die in einer Internetseite durchaus einen Sinn haben mögen, sind - wenn sie in eine HTML-Mail eingebunden sind - eher störend. In manchen Fällen werden HTML-Skripte auch aktiv dazu verwendet, Rechner zu infizieren, wobei Skripte die Möglichkeit haben, sich nicht erst durch das Öffnen einer infizierten Anlage weiterzuverbreiten, sondern alleine schon in der Vorschauansicht einer Mail wirksam werden können.

■ Anhänge filtern

Beim Filtern von Anhängen haben Sie eine große Auswahl von Möglichkeiten, um **Mail-Anhänge** (= Attachments) und Anlagen zu filtern. Die meisten E-Mailviren verbreiten sich über solche **Attachments**, die in den meisten Fällen mehr oder minder gut verborgene ausführbare Dateien enthalten. Dabei kann es sich um eine klassische EXE-Datei handeln, die ein Schadprogramm enthält, aber auch um VBS-Skripte, die sich unter bestimmten Voraussetzungen sogar hinter vermeintlich sicheren Grafik-, Film- oder Musikdateien verbergen. Generell sollte jeder Anwender bei der Ausführung von Mailanhängen große Vorsicht walten lassen und im Zweifelsfall lieber noch einmal eine Rückfrage beim Absender einer Mail durchführen, bevor er eine Datei ausführt, die er nicht ausdrücklich angefordert hat. Unter „**Dateierweiterungen**“ können Sie die **Dateiendungen** aufzählen, auf die Sie den jeweiligen Filter anwenden möchten. Dabei können Sie z.B. alle ausführbaren Dateien (z.B. EXE und COM-Dateien) in einem Filter zusammenfassen, aber auch andere Formate (z.B. MPEG, AVI, MP3, JPEG, JPG, GIF etc.) filtern, wenn diese aufgrund Ihrer Größe eine Belastung für den Mailserver darstellen. Selbstverständlich können Sie auch beliebige Archivdateien (z.B. ZIP, RAR oder CAB) filtern. Trennen Sie bitte alle Dateierweiterungen einer Filtergruppe durch Semikolon, z.B. „*.exe;*.dll“. Über die Funktion „**Auch Anhänge in eingebetteten Mails filtern**“ sorgen Sie dafür, dass die Filterung der unter „**Dateierweiterungen**“ ausgewählten Anlagentypen auch in Mails stattfindet, die selber eine Anlage einer Mail darstellen. Diese Option sollte generell aktiviert sein. Über „**Anhänge nur umbenennen**“ werden die zu filternden Anlagen nicht automatisch gelöscht, sondern nur umbenannt. Dies ist z.B. bei ausführbaren Dateien (wie z.B. EXE und COM) durchaus sinnvoll, aber auch bei Microsoft Office-Dateien, die möglicherweise ausführbare Scripte und **Makros** enthalten könnten. Durch das Umbenennen einer Anlage kann Sie nicht unbeachtet durch einfachen Mausklick geöffnet werden, sondern muss vom Empfänger erst abgespeichert und ggf. wieder umbenannt werden, bevor er sie verwenden kann. Wenn das „**Häkchen bei Anhängen nur umbenennen**“ nicht gesetzt ist, werden die entsprechenden Anhänge direkt gelöscht. Unter „**Suffix**“ geben Sie die Zeichenfolge ein, mit der Sie die eigentliche Dateiendung erweitern möchten, auf diese Weise wird die Ausführbarkeit einer Datei durch einfaches Anklicken verhindert (z.B. „*.exe.danger“). Unter „**Meldung im Text der Mail einfügen**“ können Sie den Empfänger der gefilterten Mail darüber informieren, dass ein Anhang aufgrund einer Filterregel gelöscht oder umbenannt wurde.

■ Inhaltsfilter

Über den Inhaltsfilter können Sie E-Mails, die bestimmte Themen oder Texte enthalten auf bequeme Weise blocken. Geben Sie dazu unter „**Suchkriterium**“ einfach die **Schlüsselwörter** und **Ausdrücke** ein, auf die AntiSpam reagieren soll. Dabei können Sie Text auf beliebige Weise mit den logischen **Operatoren** UND und ODER verknüpfen.

■ Wenn Sie z.B. **sex**, „**ODER**“ **drugs**, „**ODER**“ **rock'n'roll** eingeben „**UND**“ **wein**, „**ODER**“ **weib**, „**ODER**“ **gesang**, würde der Filter bei einer Mail, die z.B. die Begriffe „**drugs**“ und „**wein**“ enthält, aktiviert werden, nicht aber bei einer Mail, die nur den Begriff „**drugs**“ oder nur den Begriff „**wein**“ enthält. Der logische Operator „**UND**“ setzt also voraus, dass alle mit „**UND**“ verknüpften Elemente vorhanden sind, der logische Operator „**ODER**“ setzt lediglich voraus, dass ein Element vorhanden ist.

Geben Sie nun unter „**Suchbereich**“ an, in welchen Bereichen einer Mail nach diesen Ausdrücken gesucht werden soll. Als „**Header**“ wird der Bereich einer Mail bezeichnet, der unter anderem die E-Mail-Adresse des Absenders und des Empfängers, die Betreffzeile und Informationen zu den verwendeten Programmen, Protokollen und Absendedaten enthält. Im Unterschied dazu wird mit „**Betreff**“ nur der Inhalt der Betreffzeile ohne weitere Textinformationen aus dem Header überprüft. Beim „**Mailtext**“ haben Sie zudem die Auswahl, ob sich der Suchbereich nur auf reine **Text-Mails** oder auch auf den Text in **HTML-Mails** („**HTML-Text**“) erstreckt. Über „**Eingebettete Mails**“ können Sie festlegen, ob die Suche des Inhaltsfilters sich auch auf Mails erstreckt, die in der empfangenen Mail als Anlage vorhanden sind. Unter „**Reaktion**“ können Sie festlegen, wie mit Mails verfahren werden soll, die von AntiSpam als Spam erkannt wurden. Über „**Mail zurückweisen**“ wird die betreffende Mail von Ihrem E-Mailprogramm erst gar nicht in Empfang genommen, wenn Sie das Häkchen bei „**Warnung in Betreff und Text der Mail einfügen**“ setzen, können Sie dem eigentlichen Text der Betreffzeile eine Warnung voranstellen („**Prefix in Betreffzeile**“), z.B. „**SPAM**“ oder „**ACHTUNG**“. Wahlweise können Sie auch einen Text eingeben, der bei Spam-Verdacht dem eigentlichen Mailtext vorangestellt wird („**Meldung in Text**“). Wenn Sie **Microsoft Outlook** verwenden (Achtung: Nicht zu verwechseln mit **Outlook Express**), haben Sie auch die Möglichkeit, Mails mit **Spamverdacht** in einem frei definierbaren Ordner in Ihrem Postfach zu verschieben („**Mail in Ordner verschieben**“). Sie können diesen Ordner direkt über AntiSpam anlegen, in dem Sie unter „**Ordnername**“ den entsprechenden Ordner definieren.

■ Absenderfilter

Über den Absenderfilter können Sie E-Mails, die von bestimmten Absendern kommen, auf bequeme Weise blocken. Geben Sie dazu unter „**Adressen/Domains**“ einfach die **E-Mail-Adressen** oder **Domain-Namen** ein, auf die AntiSpam reagieren soll. Mehrere Einträge können Sie durch **Semikolon** voneinander trennen. Unter „**Reaktion**“ können Sie festlegen, wie mit Mails verfahren werden soll, die von AntiSpam als Spam erkannt wurden. Über „**Mail zurückweisen**“ wird die betreffende Mail von Ihrem E-Mailprogramm erst gar nicht in Empfang genommen, wenn Sie das Häkchen bei „**Warnung in Betreff und Text der Mail einfügen**“ setzen, können Sie dem eigentlichen Text der Betreffzeile eine Warnung voranstellen („**Prefix in Betreffzeile**“), z.B. „**SPAM**“ oder „**ACHTUNG**“. Wahlweise können Sie auch einen Text eingeben, der bei Spam-Verdacht dem eigentlichen Mailtext vorangestellt wird

(„**Meldung in Text**“). Wenn Sie **Microsoft Outlook** verwenden (Achtung: Nicht zu verwechseln mit **Outlook Express**), haben Sie auch die Möglichkeit, Mails mit **Spamverdacht** in einem frei definierbaren Ordner in Ihrem Postfach zu verschieben („**Mail in Ordner verschieben**“). Sie können diesen Ordner direkt über AntiSpam anlegen, in dem Sie unter „**Ordnername**“ den entsprechenden Ordner definieren.

■ Sprachenfilter

Mit dem **Sprachenfilter** können Sie automatisch Mails bestimmter Landessprachen als Spam definieren. Wenn Sie also in der Regel z.B. keinen Mailkontakt zu englischsprachigen Personen haben, können Sie über die Definierung von Englisch als Spam-Sprache sehr viele Spams ausfiltern. Wählen Sie hier einfach die Sprachen aus, bei denen Sie davon ausgehen, dass Sie in eben diesen Sprachen keine regulären Mails erhalten und AntiSpam erhöht damit die Spameinschätzung für diese Mails erheblich. Über den Bereich „**Reaktion**“ können Sie festlegen, wie mit entsprechend gefilterten Mails verfahren werden soll.

■ Statistik

Im Statistik-Bereich erhalten Sie eine ausführliche statistische Auswertung der Spam-relevanten Vorgänge auf Ihrem Mail-Server. Über den **Aktualisieren**-Button können Sie den aktuellsten Datenstand von AntiSpam abrufen, über den **Zurücksetzen**-Button löschen Sie alle bisher aufgeführten statistischen Angaben.

Spam-Filter Statistik	
Statistik	
Statistik seit	07.02.2008 14:28:39
Mails bearbeitet	0
Filter angewendet	0
davon Spamverdacht	0
davon hohe Wahrscheinlichkeit	0
davon sehr hohe Wahrscheinlichkeit	0

■ Kein Spam

Hier erhalten Sie eine ausführliche Übersicht über alle Mails, die von AntiSpam nicht als Spam definiert wurden. Über den **Aktualisieren**-Button können Sie den aktuellsten Datenstand von AntiSpam abrufen. Die eigentlichen Mails in ihrem Mailprogramm werden dabei natürlich nicht (!) gelöscht.



Über den Button „**Auf Whitelist**“ können Sie eine oder mehrere markierte Mails auf die Whitelist setzen und damit die betreffenden Mailadressen generell von einer weiteren Spamprüfung ausschließen. Lesen Sie hierzu bitte auch den Abschnitt „**Whitelist**“ im Kapitel „**Spam-Filter**“. Über den Button „**Auf Blacklist**“ können Sie eine oder mehrere markierte Mails auf die Blacklist setzen und damit die betreffenden Mailadressen generell besonders auf Spam-Elemente überprüfen. Lesen Sie hierzu bitte auch den Abschnitt „**Blacklist**“ im Kapitel „**Spam-Filter**“.

■ Spam

Hier erhalten Sie eine ausführliche Übersicht über alle Mails, die von AntiSpam als Spam definiert wurden. Über den **Aktualisieren**-Button können Sie den aktuellsten Datenstand von AntiSpam abrufen, über den **Löschen**-Button löschen Sie alle bisher markierten Einträge. Die eigentlichen Mails in ihrem Mailprogramm werden dabei natürlich nicht (!) gelöscht.



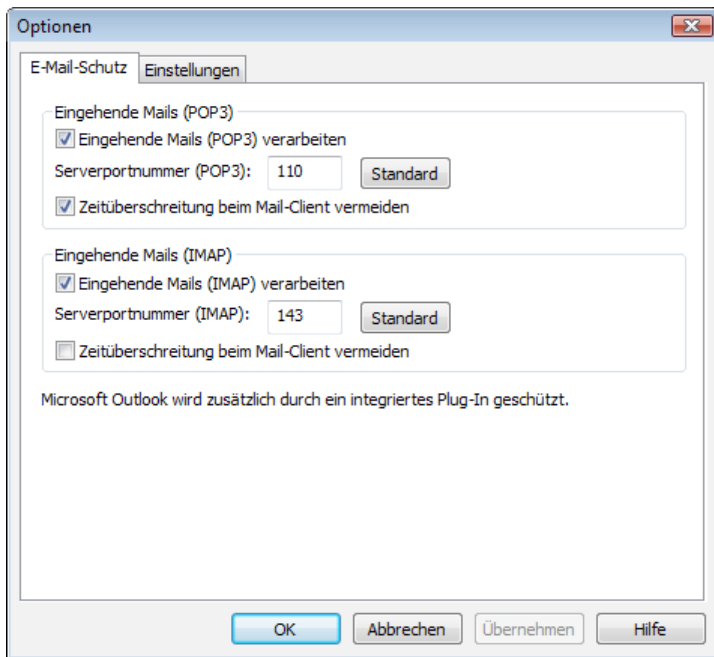
Über den Button „**Auf Whitelist**“ können Sie eine oder mehrere markierte Mails auf die Whitelist setzen und damit die betreffenden Mailadressen generell von einer weiteren Spamprüfung ausschließen. Lesen Sie hierzu bitte auch den Abschnitt „**Whitelist**“ im Kapitel „**Spam-Filter**“. Über den Button „**Auf Blacklist**“ können Sie eine oder mehrere markierte Mails auf die Blacklist setzen und damit die betreffenden Mailadressen generell besonders auf Spam-Elemente überprüfen. Lesen Sie hierzu bitte auch den Abschnitt „**Blacklist**“ im Kapitel „**Spam-Filter**“.

■ Optionen

Im Optionen-Bereich können Sie grundlegende Einstellungen der Software verändern. Klicken Sie dazu einfach die Registerkarte mit den jeweiligen Einstellungsoptionen an.

■ E-Mail-Schutz

AntiSpam schützt nach der Installation automatisch Ihre **POP3/IMAP-basierten E-Mail-Postfächer** (wie z.B. Outlook Express, Pegasus, Opera etc.) vor Spam. Dazu verwendet es einen speziellen Client, der die Mails überprüft, bevor Sie von Ihrem E-Mail-Programm empfangen bzw. versendet werden.



Durch Setzen der jeweiligen Häkchen können Sie den Schutz für **eingehende Mails (POP3)** und **eingehende Mails (IMAP)** auch abschalten.

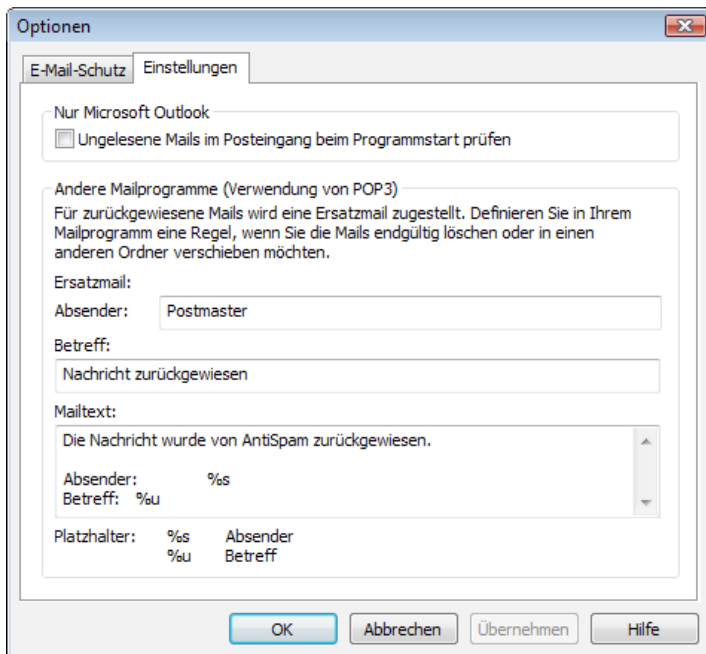
- Wenn Sie bei der Nutzung Ihrer E-Mail-Programme nicht die Standardports verwenden, können Sie unter „Serverportnummer“ auch den Port angeben, den Sie für eingehende oder ausgehende Mails verwenden. Mit Anklicken des Standard-Buttons können Sie automatisch die Standardportnummern wiederherstellen.
- Microsoft Outlook wird durch ein spezielles PlugIn geschützt. Lesen Sie hierzu bitte auch das Kapitel „Optionen > Einstellungen“.

■ Zeitüberschreitung beim Mail-Programm vermeiden

Da das AntiSpam die eingehenden Mails zeitlich vor dem eigentlichen Mailprogramm bearbeitet, kann es bei großen Mail-Mengen oder langsamen Verbindungen vorkommen, dass eine Fehlermeldung beim Mailprogramm erscheint, weil es nicht sofort die Maildaten zugestellt bekommt, da diese ja von AntiSpam auf Spamverdacht überprüft werden. Mit Anklicken dieses Häkchenfeldes wird eine solche Fehlermeldung des Mailprogramms unterdrückt und sobald sämtliche Maildaten auf Spamverdacht überprüft wurden, werden diese von AntiSpam dann ganz normal an das Mailprogramm weitergereicht.

■ Einstellungen

In diesem Bereich haben Sie die Möglichkeit, weitere Einstellungen vorzunehmen.



■ Ungelesene Mails beim Programmstart prüfen

Nur für Microsoft Outlook: Diese Option dient dazu, E-Mails auf Spamverdacht zu kontrollieren, die Sie erreichen, während Sie nicht mit dem Internet verbunden sind. Sobald Sie **Outlook** öffnen, werden deshalb sämtliche ungelesenen Mails im Posteingang-Ordner und den darin enthaltenen Unterordnern von AntiSpam kontrolliert.

■ Andere Mailprogramme (Verwendung von POP3)

Über **POP3** empfangene Mails können aus technischen Gründen nicht direkt gelöscht werden. Wenn ein Filter Mails zurückweisen soll, wird diese Mail dann mit einem Ersatztext versehen. Der Ersatztext bei zurückgewiesenen Mails lautet dabei: **„Die Nachricht wurde vom AntiSpam zurückgewiesen“**.

Sie können den Text für diese Benachrichtigungsfunktionen aber auch individuell gestalten. Im frei definierbaren Text für den Betreff und den Mailtext stehen Ihnen folgende Platzhalter (definiert durch ein Prozentzeichen mit einem anschließenden Kleinbuchstaben) zur Verfügung:

%s Absender
%u Betreff

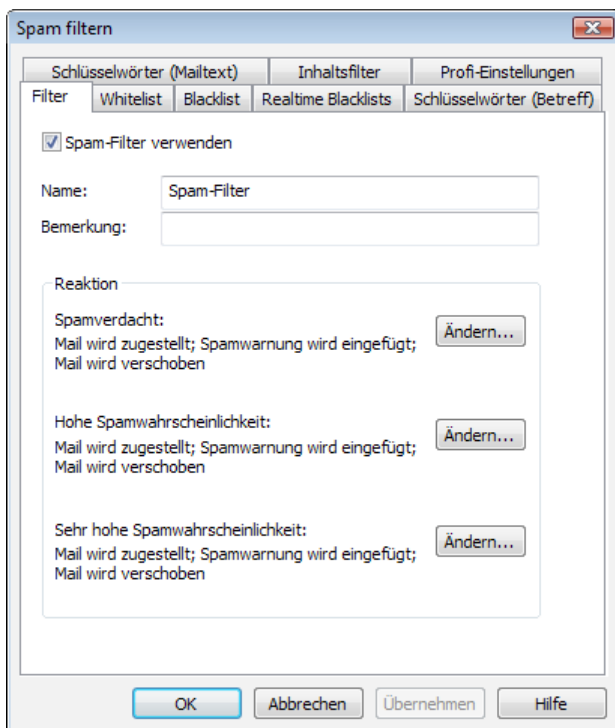
■ Sie können in Ihrem Mailprogramm eine Regel definieren, die Mails mit dem hier definierten Ersatztext automatisch löscht.

■ Spam-Filter

Über den Spam-Filter haben Sie umfangreiche Einstellungsmöglichkeiten, um Mails mit unerwünschten Inhalten oder von unerwünschten Absendern (z.B. Massenmailversendern) wirkungsvoll zu blockieren. Das Programm prüft viele Merkmale der Mails, die typisch für Spam sind. Anhand der zutreffenden Merkmale wird ein Wert errechnet, der die Wahrscheinlichkeit für Spam widerspiegelt. Dazu stehen Ihnen mehrere Karteikarten zur Verfügung, in denen Ihnen alle relevanten Einstellungsmöglichkeiten thematisch gegliedert zur Verfügung stehen.

■ Filter

Geben Sie unter **„Name“** und **„Bemerkung“** an, wie Sie den Filter nennen möchten und welche zusätzlichen Informationen hierzu vielleicht nötig sind. Unter **„Reaktion“** können Sie bestimmen, wie der Spam-Filter mit Mails umgehen soll, die möglicherweise Spam enthalten. Dabei können Sie drei Abstufungen vornehmen, die davon beeinflusst werden, wie hoch AntiSpam die Wahrscheinlichkeit dafür ansetzt, dass es sich bei der betreffenden E-Mail um Spam handelt. Unter **„Spamverdacht“** wird der Umgang mit den Mails geregelt, in denen AntiSpam einzelne Spam-Elemente findet. Dabei muss es sich nicht generell um Spam handeln, sondern in seltenen Fällen möglicherweise auch um Newsletter-Mails oder Sammelmailings, die vom Empfänger durchaus erwünscht sind. Hier empfiehlt es sich, den Empfänger auf den Spam-Verdacht hinzuweisen. Unter **„Hohe Spamwahrscheinlichkeit“** werden die Mails zusammengefasst, die viele Merkmale für Spam in sich vereinen und nur in sehr seltenen Fällen vom Empfänger wirklich erwünscht sind. Unter **„Sehr hohe Spamwahrscheinlichkeit“** finden sich die Mails, die alle Kriterien einer Spam-Mail erfüllen. Hier handelt es sich so gut wie nie um gewünschte E-Mails und das Zurückweisen von derart gestalteten Mails ist in den meisten Fällen empfehlenswert. Jede dieser drei abgestuften Reaktionen können Sie individuell gestalten. Klicken Sie dazu einfach auf den **Ändern**-Button und definieren die Reaktion, mit der AntiSpam reagieren soll. So haben Sie über **„Mail zurückweisen“** die Möglichkeit, die Mail gar nicht erst in Ihr Postfach gelangen zu lassen. Über **„Spamwarnung in Betreff und Text der Mail einfügen“** können Sie als Spam identifizierten Mails auch als solche auffällig kennzeichnen, um sie z.B. besser aussortieren zu können.



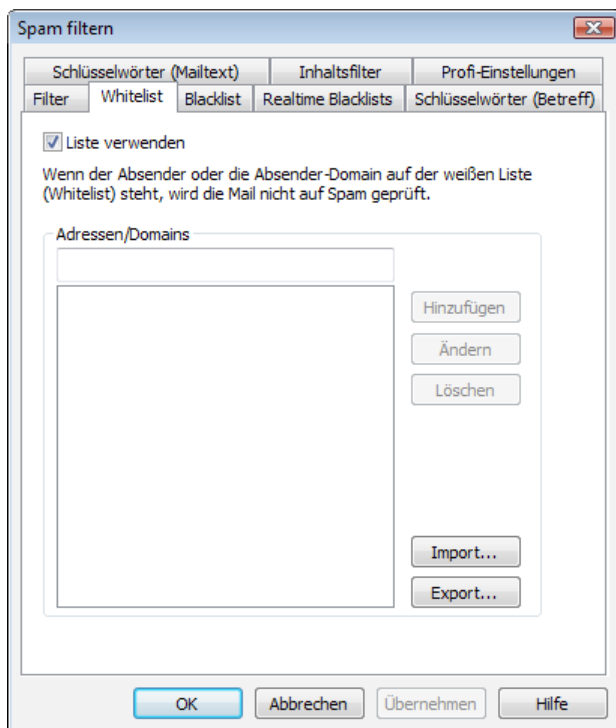
Wenn Sie Microsoft Outlook verwenden (Achtung: Nicht zu verwechseln mit Outlook Express), haben Sie auch die Möglichkeit, Mails mit Spamverdacht in einem frei definierbaren Ordner in Ihrem Postfach zu verschieben („**Mail in Ordner verschieben**“). Sie können diesen Ordner direkt über AntiSpam anlegen, in dem Sie unter „**Ordnername**“ den entsprechenden Ordner definieren.

■ Auch wenn Sie kein Outlook verwenden, können Sie die als Spam erkannten Mails in einen Ordner verschieben lassen. Fügen Sie dazu eine Warnung in die Betreffzeile ein (z.B. „[SPAM]“) und erstellen Sie in Ihrem Mailprogramm eine Regel, die Mails mit dem Text in der Betreffzeile in einen anderen Ordner verschiebt.

■ Whitelist

Über die Whitelist können Sie bestimmte Absender-Adressen oder Domains explizit vom Spamverdacht ausnehmen. Geben Sie dazu einfach in das Feld „**Adressen/ Domains**“ die gewünschte E-Mail-Adresse (z.B. newsletter@gdata.de) oder **Domain**

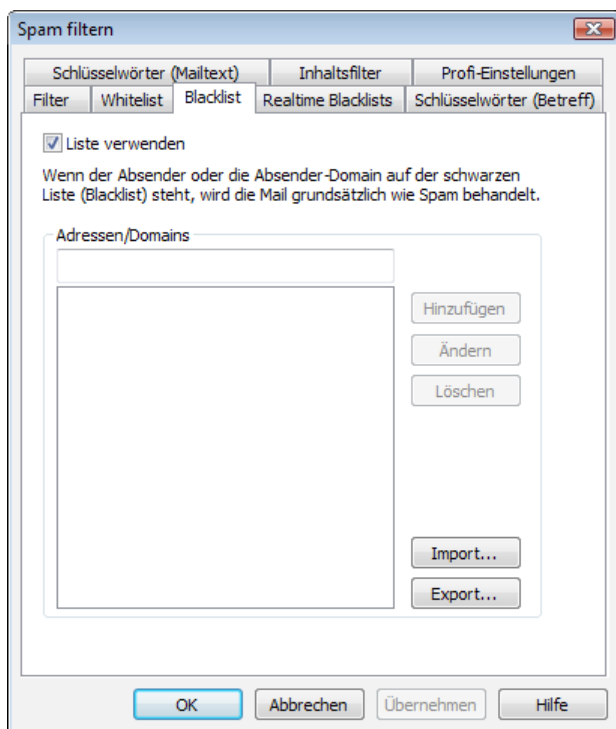
(z.B. gdata.de) ein, die Sie vom **Spamverdacht** ausnehmen möchten und AntiSpam behandelt Mails von diesem Absender bzw. dieser **Absenderdomain** nicht als Spam. Über den **Import**-Button können Sie auch vorgefertigte Listen von E-Mail-Adressen oder Domains in die Whitelist einfügen. Die Adressen und Domains müssen in so einer Liste in einzelnen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache txt-Datei verwendet, wie sie z.B. auch mit dem Windows **Notepad** erstellt werden kann. Über den **Export**-Button können Sie eine solche Whitelist auch als **Textdatei** exportieren.



■ Blacklist

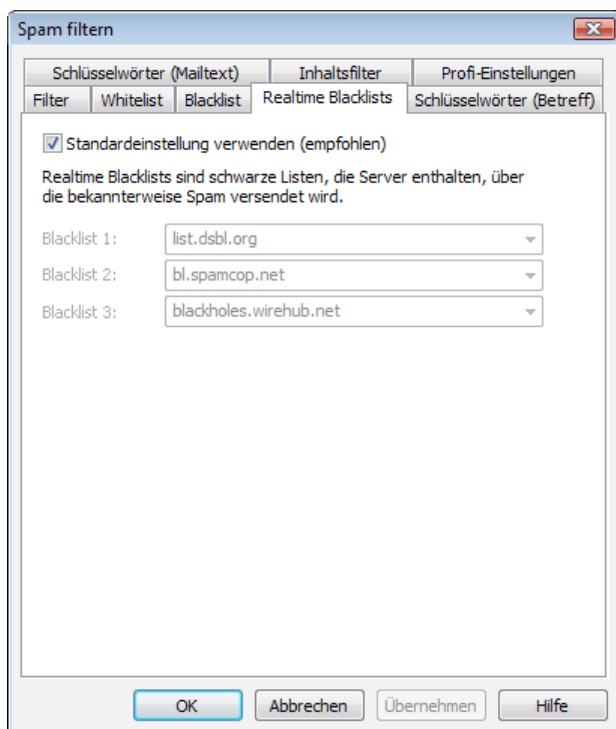
Über die Blacklist können Sie bestimmte **Absender-Adressen** oder **Domains** explizit unter Spamverdacht setzen. Geben Sie dazu einfach in das Feld „**Adressen/ Domains**“ die gewünschte E-Mail-Adresse (z.B. newsletter@megaspam.de.vu) oder Domain (z.B. megaspam.de.vu) ein, die Sie unter **Spamverdacht** setzen möchten und AntiSpam behandelt Mails von diesem Absender bzw. dieser Absenderdomain generell als „**Mails mit sehr hoher Spamwahrscheinlichkeit**“. Über den **Import**-Button können Sie auch vorgefertigte Listen von E-Mail-Adressen oder Domains in die Blacklist einfügen. Die Adressen und Domains müssen in so einer Liste in ein-

zelenen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache txt-Datei verwendet, wie sie z.B. auch mit dem Windows Notepad erstellt werden kann. Über den **Export**-Button können Sie eine solche Blacklist auch als **Textdatei** exportieren.



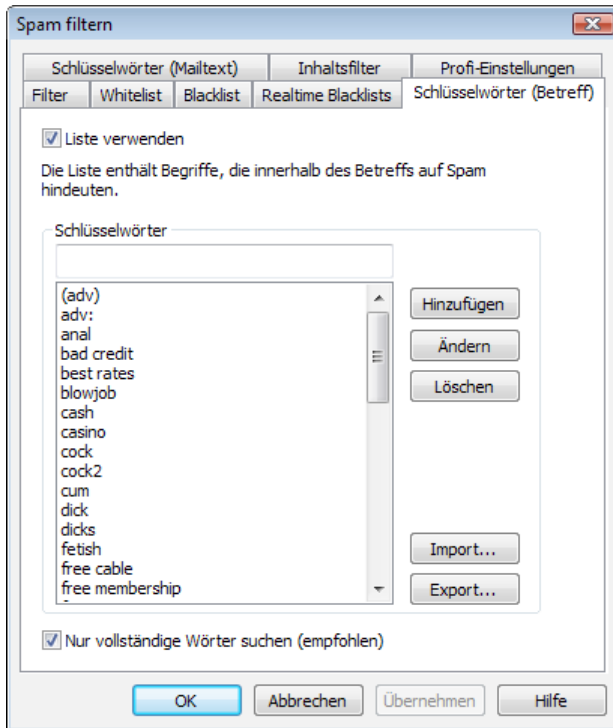
■ Realtime Blacklists

Im Internet finden sich **schwarze Listen**, die **IP-Adressen** von Servern enthalten, über die bekanntermaßen **Spam** verschickt wird. AntiSpam ermittelt durch **DNS-Anfragen** an die **RBLs (Realtime Blacklists)**, ob der sendende Server gelistet ist. Falls ja, erhöht sich die **Spamwahrscheinlichkeit**. Generell sollten Sie hier die Standardeinstellung verwenden, können allerdings auch unter Blacklist 1, 2 und 3 eigene Adressen für Blacklists aus dem Internet vergeben.



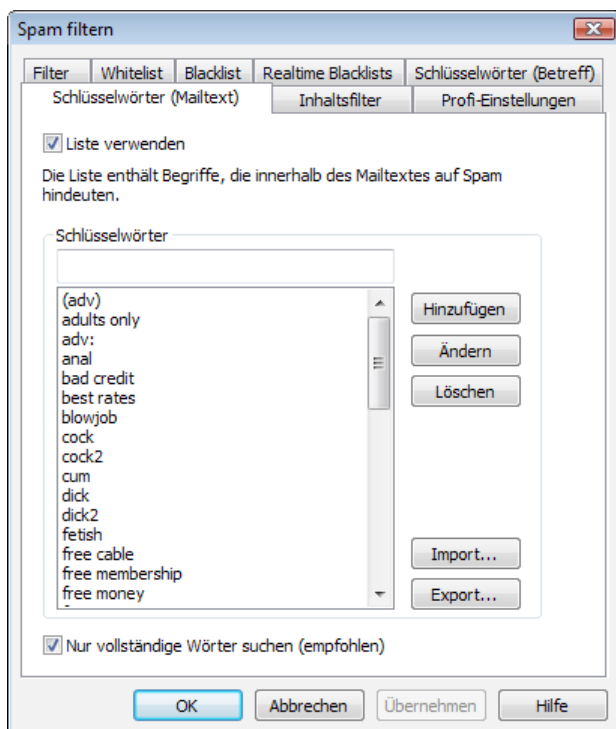
■ Schlüsselwörter (Betreff)

Über die Liste der Schlüsselwörter können Sie Mails auch anhand der in der **Betreffzeile** verwendeten Wörter unter **Spamverdacht** stellen. Wenn mindestens einer der Begriffe in der Betreffzeile vorkommt, erhöht sich die **Spamwahrscheinlichkeit**. Diese Liste können Sie über die Buttons „**Hinzufügen**“, „**Ändern**“ und „**Löschen**“ beliebig verändern. Über den **Import**-Button können Sie auch vorgefertigte Listen von Schlüsselwörtern in Ihre Liste einfügen. Die Einträge müssen in so einer Liste in einzelnen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache txt-Datei verwendet, wie sie z.B. auch mit dem Windows **Notepad** erstellt werden kann. Über den **Export**-Button können Sie eine solche Liste von Schlüsselwörtern auch als **Textdatei** exportieren. Über das Häkchen vor „**Nur vollständige Wörter suchen**“ können Sie festlegen, dass AntiSpam die Betreffzeile einer Mail nur nach ganzen Wörtern durchsucht, so würde z.B. ein Begriff wie „cash“ unter Spamverdacht fallen, während z.B. die gemeinen Cashew-Kerne weiterhin unbeanstandet bleiben.



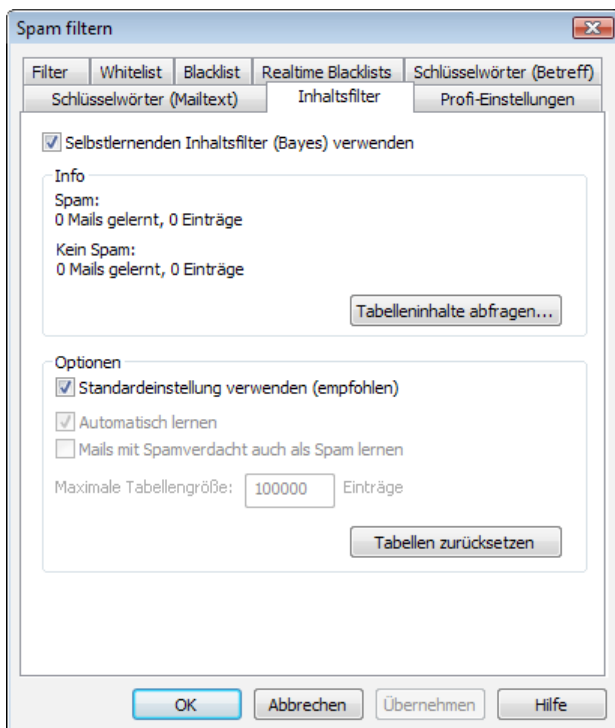
■ Schlüsselwörter (Mailtext)

Über die Liste der Schlüsselwörter können Sie Mails auch anhand der im **Mailtext** verwendeten Wörter unter **Spamverdacht** stellen. Wenn mindestens einer der Begriffe im Mailtext vorkommt, erhöht sich die **Spamwahrscheinlichkeit**. Diese Liste können Sie über die Buttons „**Hinzufügen**“, „**Ändern**“ und „**Löschen**“ beliebig verändern. Über den **Import**-Button können Sie auch vorgefertigte **Listen von Schlüsselwörtern** in Ihre Liste einfügen. Die Einträge müssen in so einer Liste in einzelnen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache txt-Datei verwendet, wie sie z.B. auch mit dem Windows **Notepad** erstellt werden kann. Über den **Export**-Button können Sie eine solche Liste von Schlüsselwörtern auch als **Textdatei** exportieren. Über das Häkchen vor „**Nur vollständige Wörter suchen**“ können Sie festlegen, dass AntiSpam die Betreffzeile einer Mail nur nach ganzen Wörtern durchsucht, so würde z.B. ein Begriff wie „cash“ unter Spamverdacht fallen, während z.B. die gemeinen Cashew-Kerne weiterhin unbeanstandet bleiben.



■ Inhaltsfilter

Beim Inhaltsfilter handelt es sich um einen **selbstlernenden Filter** auf Basis der **Bayes-Methode**, der auf Grund der im **Mailtext** verwendeten Worte eine **Spamwahrscheinlichkeit** berechnet. Dabei arbeitet dieser **Filter** nicht allein auf Basis feststehender Wortlisten, sondern lernt bei jeder neu empfangenen Mail weiter dazu. Über den Button „**Tabelleninhalte abfragen**“ können Sie sich die Wortlisten anzeigen lassen, die der Inhaltsfilter zur Einordnung einer Mail als Spam verwendet. Über den Button „**Tabellen zurücksetzen**“ löschen Sie alle gelernten Tabelleninhalte und der selbstlernende Inhaltsfilter startet den Lernvorgang erneut von Beginn an.



■ Profi-Einstellungen

In diesem Bereich können Sie die **Spamerkennung** von AntiSpam sehr detailliert verändern und an die Gegebenheiten Ihres Mailverkehrs anpassen. Generell empfiehlt es sich hier jedoch, die Standardeinstellungen zu verwenden. In den Profi-Einstellungen sollten Sie nur dann Veränderungen vornehmen, wenn Sie sich in der Thematik auskennen und genau wissen, was Sie tun.

■ Bedienung des Webfilters

Über den Webfilter können Sie bestimmen, welche Web-Elemente, die über das reine **HTTP-Protokoll** hinausgehen (also der Ansicht text- und grafikbasierter **Websites**) geblockt werden sollen. Außerdem haben Sie die Möglichkeit, **Spuren** zu löschen, die auf Ihr **Surfverhalten** im **Internet Explorer** hindeuten. Die **Bedienung des Webfilters** ist prinzipiell selbsterläuternd und übersichtlich gestaltet. Anhand unterschiedlicher Karteikarten, die Sie über die links angezeigten Symbole anwählen können, wechseln Sie in den jeweiligen Programmbereich und können dort Aktionen durchführen, Voreinstellungen vornehmen oder Vorgänge überprüfen.



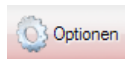
Folgende **Programmbereiche** stehen zur Verfügung

- **Web-Filter:** Über den Webfilter können Sie bestimmen, welche Web-Elemente, die über das reine HTTP-Protokoll hinausgehen (also der Ansicht text- und grafikbasierter Websites) geblockt werden sollen.
- **Spurenlöscher:** Hier haben Sie die Möglichkeit, Spuren zu löschen, die auf Ihr Surfverhalten im Internet Explorer hindeuten.
- **Whitelist:** In der Whitelist sind Webseiten aufgelistet, die von der Filterfunktion des Webfilters ausgenommen werden.

Außerdem finden Sie in der oberen Menüleiste der Programmoberfläche übergreifende Funktionen und Einstellungsmöglichkeiten.



Update-Bereich: Hier können Sie Aktualisierungen aus dem Internet überspielen. Da mit einem Update auch die Signaturen für Phishing-Sites und andere unseriöse Webangebote aktualisiert werden, empfiehlt es sich, das Update in regelmäßigen Abständen durchzuführen.



Optionen-Bereich: In den Web-Optionen können Sie bestimmen, dass sämtliche HTTP-Webinhalte schon beim Browsen auf Viren überprüft werden. Infizierte Webinhalte werden dann gar nicht erst ausgeführt und die entsprechenden Seiten nicht angezeigt. Setzen Sie hierzu bitte das Häkchen bei „**Internetinhalte (HTTP) verarbeiten**“. Wenn Sie dieses Häkchen nicht setzen, sind Webfilter, Spurenlöscher und Kindersicherung nicht aktiv. Da der Webfilter die Web-Inhalte vor Ihrer Darstellung im Internet Browser bearbeitet und dafür je nach Datenaufkommen eine gewisse Zeit benötigt, kann es vorkommen, dass eine Fehlermeldung im Internet Browser erscheint, weil dieser nicht sofort die Daten zugestellt bekommt, da diese ja auf Schadroutinen überprüft werden. Mit Aktivieren des Häkchenfeldes „**Zeitüberschreitung im Browser vermeiden**“ wird eine solche Fehlermeldung unterdrückt und sobald sämtliche Browserdaten auf Viren überprüft wurden, werden diese dann ganz normal an den Internetbrowser überreicht. Mit der „**Größenbegrenzung für Downloads**“ können Sie die HTTP-Überprüfung für zu große Webinhalte unterbrechen. Die Inhalte werden dann vom AntiVirus-Virenwächter überprüft, sobald etwaige Schadroutinen aktiv werden. Der Vorteil bei dieser Größenbegrenzung liegt darin, dass es beim Surfen im Web nicht zu Verzögerungen durch die Virenkontrolle kommt. Inhalte, die wegen Ihrer Größe nicht VOR Ihrer Anzeige im Browser auf Viren und Schadprogramme überprüft werden, werden vom Wächter natürlich spätestens dann erkannt und geblockt, wenn sie Schadroutinen ausführen möchten.

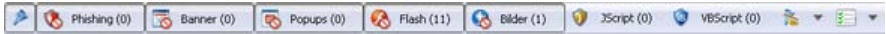


Hilfe-Bereich: Hier rufen Sie die Online-Hilfe zum Produkt auf.

Nach der Installation des Webfilters steht Ihnen im Internet Explorer außerdem eine spezielle Symbolleiste zur Verfügung, über die Sie bei der Verwendung des Browsers schnell und bequem die Filtereinstellungen für die angesurfte Seite verschärfen oder lockern können. Die Funktionalität der Symbolleiste wird Ihnen im Kapitel „**Webfilter-Symbolleiste im Internet Explorer**“ erläutert.

■ Webfilter-Symboleiste im Internet Explorer

Im **Internet Explorer** steht Ihnen nach der Installation des Webfilters auch eine spezielle **Symboleiste** zur Verfügung, mit der Sie bequem die einzelnen Webfilter-Funktionen an- oder abschalten können. Wenn an dem jeweiligen Symbol ein rotes Parkverbotsschild abgebildet ist, wird der entsprechende Inhalt geblockt.



Sie können die **Anzeige der Webfilter-Symboleiste** im Internet Explorer unter „**Ansicht > Symboleisten > G DATA WebFilter**“ ein- oder ausschalten.

Folgende Funktionen stehen Ihnen hier zur Verfügung:



WebFilter: Über diese Funktion können Sie den Webfilter komplett ein- oder ausschalten.



Phishing (0)

Phishingseiten blocken: Mit Phishing-Mails versuchen Betrüger Kunden einer bestimmten Bank oder eines Shops auf eine gefälschte Webseite zu lenken, auf der diese dann Ihre Daten eingeben sollen, welche dann missbräuchlich verwendet werden. Der Web-Filter erhält online ständig neueste Informationen über neue Phishing-Websites und unterdrückt diese automatisch. Die Aktivierung dieser Überwachungsoption ist sehr empfehlenswert.



Banner (0)

Banner blocken: Werbebanner haben meist nur eine bestimmte Anzahl unterschiedlicher Größen. Diese Bildgrößen können bei der Kontrollen von Bannern ausgefiltert werden.



Popups (0)

Popup blocken: Bei Popups handelt es sich um sich unerwünscht öffnende Webseiten in Form kleiner Werbeeinblendungen. Wenn Sie die Funktion „**Popup überwachen**“ auf aktiv schalten, werden diese Popups unterdrückt.



Flash (4)

Flash blocken: Es gibt inzwischen viele Webseiten, die Flash als Grundlage für animierte Inhalte nutzen. Auf anderen Seiten dient Flash jedoch ausschließlich zur Darstellung von animierten Werbeeinblendungen oder langwierigen Startbildschirmen (Stichwort: **Skip Intro**) ohne Informationsgehalt. Hier können Sie festlegen, ob Flashdaten angezeigt oder unterdrückt werden sollen.



Bilder (1)

Animierte Grafiken (Bilder) blocken: Sie können die Anzeige von bewegten Grafiken, also z.B. **GIF**- oder **PNG**-Bilddateien gezielt unterdrücken.



JScript blocken: **JavaScript** ist eine von Netscape entwickelte Programmiersprache, die nicht eigentlich Bestandteil von HTML ist, aber im besten Fall unterstützend dazu dient, die Darstellung und Anwenderfreundlichkeit von Webseiten zu erhöhen. Leider gibt es auch viele Web-Designer, die JavaScript für Browsereinschränkungen nutzen. Neben dem an sich harmlosen JavaScript kann der Webfilter allerdings auch aus Sicherheitsaspekten bedenkliche **JavaApplets** und **ActiveX**-Elemente blockieren.



VBScript blocken: **Visual Basic Script** ist eine speziell von Microsoft für den Internet Explorer entwickelte Technik für dynamische Elemente in Webseiten, die ähnlich wie JavaScript aufgebaut ist. Da VB-Script ausschließlich auf dem Internet Explorer funktioniert, wird es von Web-Designern eher selten verwendet. Ein Abschalten von VB-Script führt nur in den allerseltensten Fällen zu Einschränkungen beim Surfen, erhöht aber deutlich die Sicherheit.



Spurenlöscher: Wenn Sie diesen Button drücken, werden sämtliche Spuren, die Sie beim Surfen im Web hinterlassen haben, vom Rechner gelöscht. Eine Person, die den Computer nach Ihnen benutzt, kann dann also nicht mehr zurückverfolgen, auf welchen Internetseiten Sie sich befunden haben. Wenn Sie auf den Pfeilbutton rechts neben diesem Button drücken, öffnet sich eine Liste, aus der Sie gezielt die Sorte von Spuren auswählen können, die gelöscht werden sollen.

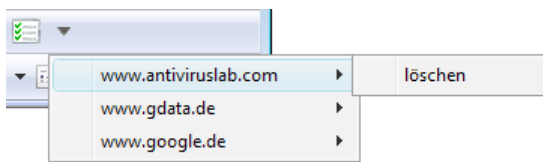
- **Temporäre Internetdateien löschen**
- **Cookies löschen**
- **Besuchte Websites löschen**
- **Zuletzt verwendete Dateien löschen**
- **Temporäre Nutzerdateien löschen**
- **Gespeicherte Formulardaten löschen**
- **Letzte Modemverbindungen löschen**
- **Verlauf aufgeführter Programme löschen**
- **Verlauf angemeldeter Nutzer löschen**
- **Verlauf gesuchter Objekte löschen**
- **Netzwerk-Verlauf löschen**

☐ *Der Spurenlöscher löscht nur die spezifischen Spuren, die Sie im Programmbereich „Spurenlöscher“ zum Löschen freigegeben haben. Wenn Sie hier also den Eintrag „Besuchte Webseiten“ auf „nicht löschen“ gestellt haben, werden diese Spuren auch nicht gelöscht.*



Die aktuelle URL der Whitelist hinzufügen: In der Whitelist können Sie vertrauenswürdige Webseiten aufnehmen, bei denen die Filterregeln des

Webfilters nicht angewendet werden, auch wenn dieser angeschaltet ist. Um die Seite, die aktuell in der Browseransicht angezeigt wird, zu dieser Whitelist hinzuzufügen, klicken Sie einfach auf diesen Button. Um die Einträge auf der Whitelist schnell und bequem wieder zu löschen, klicken Sie auf den Pfeilbutton rechts und wählen dann die Website aus, die Sie aus der Whitelist wieder löschen möchten.



■ Programmbereiche

■ Webfilter

Über den Webfilter können Sie bestimmen, welche Web-Elemente, die über das reine **HTTP-Protokoll** hinausgehen (also der Ansicht text- und grafikbasierter Websites) im Internet Explorer geblockt werden sollen. Dabei orientiert sich der Web-Filter nicht an einzelnen Benutzern, sondern beeinflusst die Anzeige von Webseiten für alle Benutzer.



Folgende Web-Filter-Einstellungen stehen Ihnen zur Verfügung:

- **WebFilter:** Über diese Funktion können Sie den Webfilter generell ein- oder ausschalten.
- **Phishingseiten blocken:** Mit Phishing-Mails versuchen Betrüger Kunden einer bestimmten Bank oder eines Shops auf eine gefälschte Webseite zu lenken, auf der diese dann Ihre Daten eingeben sollen, welche dann missbräuchlich verwendet werden. Der Web-Filter erhält online ständig neueste Informationen über neue Phishing-Websites und unterdrückt diese automatisch. Die Aktivierung dieser Überwachungsoption ist sehr empfehlenswert.
- **Banner blocken: Werbebanner** haben meist nur eine bestimmte Anzahl unterschiedlicher Größen. Diese Bildgrößen können bei der Kontrollen von Bannern ausgefiltert werden.
- **Popup blocken:** Bei Popups handelt es sich um sich unerwünscht öffnende Webseiten in Form kleiner Werbeeinblendungen. Wenn Sie die Funktion „**Popup überwachen**“ auf aktiv schalten, werden diese Popups unterdrückt.
- **Flash blocken:** Es gibt inzwischen viele Webseiten, die Flash als Grundlage für animierte Inhalte nutzen. Auf anderen Seiten dient Flash jedoch ausschließlich zur Darstellung von animierten Werbeeinblendungen oder langwierigen Startbildschirmen (Stichwort: **Skip Intro**) ohne Informationsgehalt. Hier können Sie festlegen, ob Flashdaten angezeigt oder unterdrückt werden sollen.
- **Animierte Grafiken (Bilder) blocken:** Sie können die Anzeige von bewegten Grafiken, also z.B. **GIF**- oder **PNG**-Bilddateien gezielt unterdrücken.
- **JScript blocken: JavaScript** ist eine von Netscape entwickelte Programmiersprache, die nicht eigentlich Bestandteil von HTML ist, aber im besten Fall unterstützend dazu dient, die Darstellung und Anwenderfreundlichkeit von Webseiten zu erhöhen. Leider gibt es auch viele Web-Designer, die JavaScript für Browsereinschränkungen nutzen. Neben dem an sich harmlosen JavaScript kann die Kindersicherung allerdings auch aus Sicherheitsaspekten bedenkliche **JavaApplets** und **ActiveX**-Elemente blockieren.
- **VBScript blocken: Visual Basic Script** ist eine speziell von Microsoft für den Internet Explorer entwickelte Technik für dynamische Elemente in Webseiten, die ähnlich wie JavaScript aufgebaut ist. Da VB-Script ausschließlich auf dem Internet Explorer funktioniert, wird es von Web-Designern eher selten verwendet. Ein Abschalten von VB-Script führt nur in den allerseltensten Fällen zu Einschränkungen beim Surfen, erhöht aber deutlich die Sicherheit.
- **Blocken getarnter URLs:** Unseriöse Betreiber versuchen manchmal potentielle Kunden auf Ihre Seiten zu locken, in dem Sie diese hinter getarnten **URLs** verstecken, d.h. der Link zu einer solchen Seite sieht aus, als sei er z.B. von einem seriösen Anbieter wie z.B. Microsoft, in Wirklichkeit verbirgt sich aber - hinter Zahlencodes, @-Zeichen, Fragezeichen und anderen SteuerCodes versteckt - möglicherweise eine Phishingseite. Der Webfilter erkennt Links auf **getarnte URLs** und unterbindet deren Darstellung.

■ Spurenlöcher

Im Spurenlöcher-Bereich können Sie auswählen, welche Informationen über Ihr Surfverhalten nach Beendigung Ihrer Surf-Session vom Webfilter gelöscht werden sollen. Wenn Sie Wert darauf legen, dass Ihre Ausflüge ins Internet keine Datenspuren auf dem Rechner hinterlassen, sollten Sie diese Option aktivieren.

■ *Wenn Sie nach jeder Session die Cookies löschen, passiert es bei Portal- oder Community-Seiten, dass Sie nicht automatisch erkannt werden und sich wieder mit Benutzernamen und Passwort einloggen müssen, obwohl dies vor der Benutzung des Webfilters nicht der Fall war.*



Folgende Einstellungen stehen Ihnen hier zur Verfügung:

- **Temporäre Internetdateien:** Temporärer Dateien sind Dateien, die von Programmen während ihrer Durchführung zwischengespeichert werden, um die Programmnutzung zu beschleunigen oder zu optimieren. Normalerweise werden diese Dateien nach Beenden der Software gelöscht. Beim Internet Explorer bleiben diese Dateien jedoch - je nach Einstellung der Software - bestehen, damit Internetseiten auch offline betrachtet oder bei der nächsten Auswahl schneller aufgebaut werden können. Versierte Nutzer können diese Dateien allerdings auf Ihrem Computer ausfindig machen und erhalten so einen kompletten Überblick über Ihr aktuelles Surfverhalten. Darum empfiehlt es sich, temporäre Internetdateien zu löschen, wenn der Computer von mehreren Personen genutzt wird.

- **Cookies:** Mit Cookies können Webseiten Informationen über Internetnutzer auf dessen Rechner zwischenspeichern, auslesen und verwenden. Wenn Sie z.B. von einer Website mit Namen begrüßt werden, dann hat diese Website auf Basis Ihrer vorhergehenden Angaben ein Cookie gesetzt. Die in einem Cookie erhaltenen Informationen und alleine schon der Name der Cookie-Datei, die meistens auf die jeweilige Website verweist, sind ein aussagekräftiges Indiz für Ihr Surfverhalten.
- **Besuchte Webseiten:** In der **Verlauf-** bzw. **History**-Funktion Ihres Browsers werden alle Webadressen gespeichert, die Sie besucht haben. Wenn Sie nicht möchten, dass diese Daten öffentlich werden, sollten Sie sie löschen.
- **Zuletzt verwendete Dateien:** Unter „**Start > Zuletzt verwendete Dokumente**“ werden die zuletzt von Ihnen bearbeiteten Dokumente angezeigt. Auch diese Liste kann der Spurenlöscher entfernen.
- **Temporäre Nutzerdateien:** Jeder angemeldete Benutzer unter Windows hat einen eigenen Ordner für temporäre Dateien. Normalerweise wird dieser von den Programmen geleert, die Daten darin zwischenspeichern, nach einem Programmfehler oder einem **Rechnerabsturz** kann es aber vorkommen, dass Dateien darin verbleiben.
- **Gespeicherte Formulardaten:** Der Internet Explorer kann **persönliche Informationen** speichern, um diese später in Formularen auf Webseiten wieder zur Verfügung zu stellen. Diese Option sollten Sie generell nur verwenden, wenn Sie Ihren Rechner alleine verwenden und dieser nicht von anderen Personen genutzt oder eingesehen werden kann. Hier können Sie auch diese Informationen löschen.
- **Letzte Modemverbindungen:** Windows speichert ab, wann welcher Benutzer die Modemverbindung genutzt hat.
- **Verlauf ausgeführter Programme:** Windows speichert ab, wann welcher Benutzer welches Programm zuletzt ausgeführt hat.
- **Verlauf angemeldeter Nutzer:** Windows speichert ab, wann sich die unterschiedlichen **Benutzer** eines Computers an- und abgemeldet haben.
- **Verlauf gesuchter Objekte:** Wenn Sie den Windows Such-Dialog verwenden, merkt sich Windows die vorhergehenden **Sucheinstellungen**. Mit dem Spurenlöscher können Sie diese Informationen löschen.
- **Netzwerk-Verlauf:** Analog zur **Modemverbindung** merkt sich Windows auch, welcher Benutzer wann Zugriff aufs Netzwerk (intern oder auch z.B. per **DSL**) hatte.

■ Whitelist

In der Whitelist können Sie vertrauenswürdige Webseiten aufnehmen, bei denen die Filterregeln des Webfilters nicht angewendet werden, auch wenn dieser angeschaltet ist.



Um eine neue Seite zu dieser Liste hinzufügen, klicken Sie einfach auf den **Neu**-Button und geben dann die gewünschte Internetadresse ggf. mit einer erläuternden Bemerkung ein.

- Über den **Löschen**-Button können Sie auf der Whitelist eingetragene Seiten auch wieder von der Whitelist entfernen. Diese werden dann wie alle anderen Websites von den Filterregeln des Webfilters beeinflusst.

Die Bedienung der Software

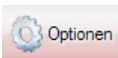
Die **Bedienung der Kindersicherung** ist prinzipiell selbsterläuternd und übersichtlich gestaltet. Anhand unterschiedlicher Karteikarten, die Sie über die links angezeigten Symbole anwählen können, wechseln Sie in den jeweiligen Programmbereich und können dort Aktionen durchführen, Voreinstellungen vornehmen oder Vorgänge überprüfen.



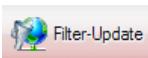
Folgende Programmbereiche stehen zur Verfügung

- **Benutzer:** Hier können Sie als Administrator Benutzerkonten verwalten und so z.B. ihren Kindern unterschiedliche Sicherheitsstufen fürs Internet zuweisen.
- **Eigene Filter:** Hier können Sie erlaubte Inhalte und verbotene Inhalte für die unterschiedlichen Benutzer individuell konfigurieren.
- **Protokoll:** Im Protokoll erhalten Sie Informationen zum Surfverhalten der jeweiligen Benutzer und können so z.B. nachvollziehen, wann die Kindersicherung auf Basis welcher Regelungen eingegriffen hat.

Außerdem finden Sie in der oberen Menüleiste der Programmoberfläche übergreifende Funktionen und Einstellungsmöglichkeiten.



Optionen: Hier können Sie grundlegende Einstellungen zum Betrieb der Kindersicherung verändern und an individuelle Bedürfnisse anpassen.



Filter-Update: Hier können Sie aktuelle Filter aus dem Internet laden, die sich thematisch damit beschäftigen, spezielle Inhalte zu blocken (Drogen, Gewalt, Pornografie etc.) oder zu erlauben (TV, Wissen, Kunst, Natur etc.). Klicken Sie einfach diesen Button an und Sie können das Filter-Update durchführen. Dazu muss natürlich eine Internetverbindung bestehen.



Testen...: Hier können Sie als Administrator überprüfen, ob Ihre Einschränkungen für bestimmte Benutzer den gewünschten Effekt haben. Im Test-Modus können Sie probeweise mit Ihrem Internetbrowser Seiten anwählen, die gesperrt sein müssten und sich so von der Korrektheit der Einstellungen überzeugen.



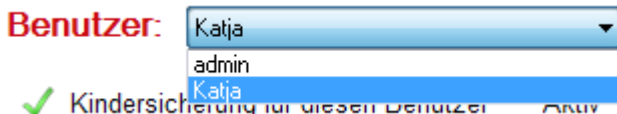
Hilfe-Bereich: Hier rufen Sie die Online-Hilfe zum Produkt auf.

■ Programmbereiche

■ Benutzer

Im Benutzer-Bereich können sie als Administrator unter "**Benutzer**" den Benutzer auswählen, für den Sie Änderungen und Einstellungen vornehmen möchten, außerdem können Sie hier neue Benutzer anlegen.

■ *Benutzer, für die auf Ihrem Computer ein Windows-Benutzerprofil besteht, können Sie unter „Benutzer“ direkt auswählen. Um hier Einstellungen zu verändern, wählen Sie einfach den gewünschten Benutzer aus und klicken dann auf den Bearbeiten-Button.*





■ Neuen Benutzer anlegen

Klicken Sie auf den Button **“Neuer Benutzer”**. Es öffnet sich eine Dialogbox, in der Sie den Benutzernamen und das Passwort für diesen Benutzer eingeben können.

- *Ein Passwort sollte im Hinblick auf Sicherheitsaspekte mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben, sowie Zahlen enthalten und, z.B. „Svenja13“ oder „Matthias12“.*

Nun erscheint unter **„Benutzer“** der neu angelegte Benutzername, gleichzeitig wird ein **Windows-Benutzerkonto** für diesen Benutzer angelegt. Das bedeutet, dass die Kindersicherung automatisch für die Person mit den jeweiligen Einstellungen aktiv ist, die sich mit ihrem Benutzernamen beim Start von Windows anmeldet.

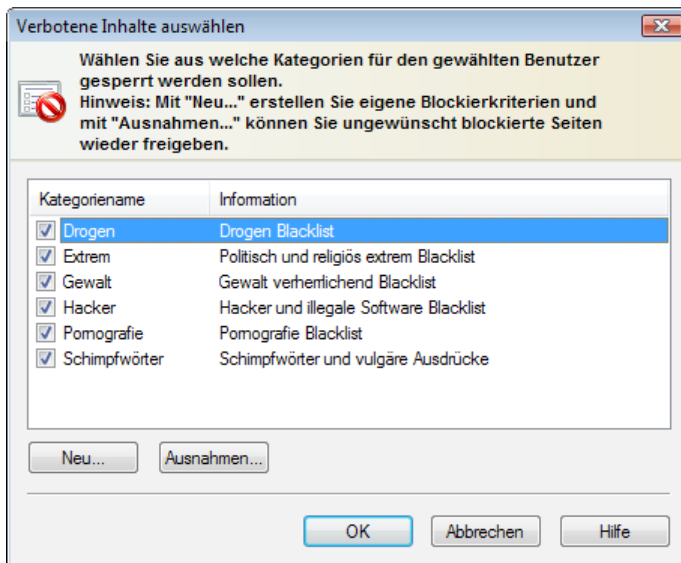


Führen Sie jetzt einen Doppelklick mit der Maus auf den Einstellungsbereich aus, der für diesen Benutzer eingestellt werden soll, also z.B. die Unterbindung „**Verbotener Inhalte**“ oder die ausschließliche Bereitstellung „**Erlaubter Inhalte**“ oder legen Sie fest, ob für diesen Benutzer die **Internetnutzungszeit** oder **Computernutzungszeit** überwacht werden soll.

■ **Verbotene Inhalte**

Über **Verbotene Inhalte** wird ein Dialogfenster geöffnet, in dem Sie für den aktuell angezeigten Benutzer spezielle Inhalte im Internet blockieren können. Wählen Sie dazu die gewünschten Kategorien, die geblockt werden sollen durch Setzen eines Häkchens aus. Klicken Sie nun auf „**OK**“ und die Internetseiten, die den Blockierkriterien entsprechen sind damit gesperrt.

- *Wenn Sie den Neu-Button anklicken, öffnet sich ein Dialogfenster, in dem Sie eigene Blockierkriterien (auch Blacklists genannt) definieren können. Definieren Sie dazu erst den Namen und ggf. einen Informationstext zum individuell erzeugten Filter.*



Wenn Sie nun auf OK klicken, öffnet sich ein weiteres Fenster, indem Sie Inhalte zusammenfassen können, die durch diesen Filter unterdrückt werden sollen. Geben Sie dazu unter „**Filter**“ einen Begriff ein, der blockiert werden soll und unter „**Ort der Suche**“ den Bereich einer Website, in dem danach gesucht werden soll. Hier haben Sie folgende Auswahlmöglichkeiten:

- **URL:** Wenn Sie das Häkchen bei „**URL**“ setzen, wird der zu blockierende Text in der Webadresse gesucht. Wenn Sie z.B. Seiten unterbinden wollen, die z.B. „www.chatcity.no“; „www.crazychat.co.uk“ o.ä. lauten, reicht es, wenn Sie als Filter „chat“ eingeben, das Häkchen bei „URL“ setzen und dann auf den **Hinzufügen**-Button klicken. Es werden nun alle Seiten blockiert, die im Domainnamen, also der Internetadresse irgendwie die Buchstabenfolge „chat“ verwenden.
- **Titel:** Wenn Sie das Häkchen bei „**Titel**“ setzen, wird der zu blockierende Text im Titel der Website gesucht. Dies ist der Bereich, den Sie z.B. sehen, wenn Sie eine Seite in Ihrer Favoritenliste als Lesezeichen „bookmarken“ möchten. Wenn Sie Seiten unterbinden wollen, die z.B. „Chat City Buxtehude“; „Teenagerchat 2005“ o.ä. lauten, reicht es, wenn Sie als Filter „chat“ eingeben, das Häkchen bei „**Titel**“ setzen und dann auf den **Hinzufügen**-Button klicken. Es werden nun alle Seiten blockiert, die im Titel irgendwie die Buchstabenfolge „chat“ verwenden.
- **Meta:** Die sogenannten Metatags sind verborgene Texteinträge auf Websites, die dazu dienen, diese in Suchmaschinen sinnvoller oder einfach auch nur häufiger zu listen. Suchbegriffe wie „sex“ oder „chat“ werden hier gerne verwendet, um die Seitenzugriffe zu erhöhen. Wenn Sie Seiten unterbinden wollen, die im Metatag irgendwo „chat“ stehen haben, reicht es, wenn Sie als Filter „chat“

eingeben, das Häkchen bei „**Meta**“ setzen und dann auf den **Hinzufügen**-Button klicken. Es werden nun alle Seiten blockiert, die in den Metatags irgendwie die Buchstabenfolge „chat“ verwenden.

- **Im gesamten Text:** Wenn Sie den lesbaren Inhalt einer Seite direkt auf zu blockierende Inhalte überprüfen möchten, geben Sie einfach den zu blockierenden Begriff - z.B. „chat“ - ein, setzen das Häkchen bei „**Im gesamten Text**“ und dann auf den **Hinzufügen**-Button klicken. Es werden nun alle Seiten blockiert, die im angezeigten Seitentext irgendwie die Buchstabenfolge „chat“ enthalten.

Natürlich kann es passieren, dass durch zu allgemein gehaltene Filterbegriffe auch Seiten blockiert werden, die an sich harmlos sind. So würde bei einem zu blockierenden Begriff wie z.B. „chat“ auch eine Seite blockiert, die sich mit „Achaten“ (also Halbedelsteinen) beschäftigt. Der Filter erkennt in „Achat“ nämlich „A-chat“ und sorgt so für eine Blockade.

☐ *Sie können spezielle Seiten, die aus Versehen in den Filterbereich fallen, aber durch die Ausnahmen-Funktion explizit wieder freischalten. Klicken Sie dazu einfach auf den Ausnahme-Button und geben in dem dortigen Filter „achat“ als Ausnahme an.*

☐ *Selbst erstellte Filter können Sie im Bereich „Eigene Filter“ beliebig bearbeiten und ggf. auch löschen. Lesen Sie hierzu das Kapitel „Eigene Filter“.*

■ Erlaubte Inhalte

Über **Erlaubte Inhalte** wird ein Dialogfenster geöffnet, in dem Sie für den aktuell angezeigten Benutzer spezielle Inhalte im Internet erlauben können. Wählen Sie dazu die gewünschten Kategorien, die erlaubt werden sollen durch Setzen eines Häkchens aus. Klicken Sie nun auf „**OK**“ und die Internetseiten, die den gewünschten Kriterien entsprechen sind damit erlaubt.

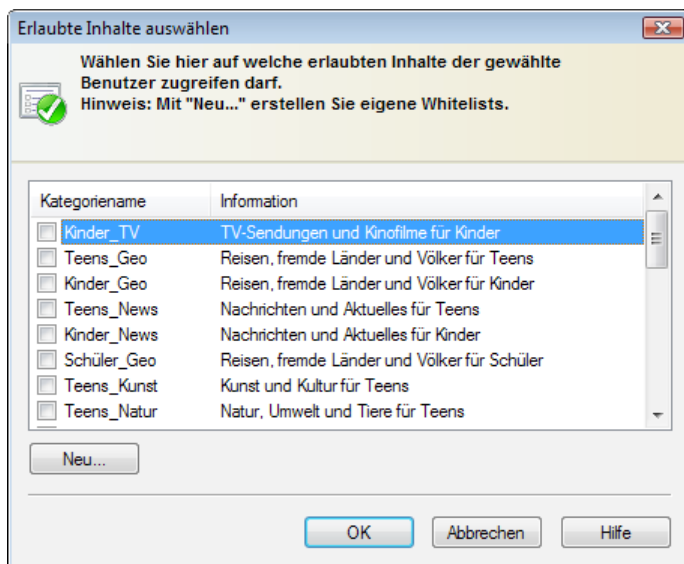
☐ *Wenn Sie den Neu-Button anklicken, öffnet sich ein Dialogfenster, in dem Sie eigene zu erlaubende Inhalte (auch Whitelists genannt) definieren können. Definieren Sie dazu erst den Namen und ggf. einen Informationstext zum individuell erzeugten Filter.*

Klicken Sie nun auf OK. Es öffnet sich ein Dialog, in dem Sie die Whitelist mit Webseiten füllen können, die z.B. kindgerecht sind.

Geben Sie dazu unter „**Filter**“ ein, welche Domainnamensbestandteile erlaubt sein sollen. Wenn Sie z.B. die Webseite des Kinderkanal freigeben wollen, können Sie hier z.B. „www.kika.de“ eingeben und erlauben damit den Zugriff auf diese Webseite. Geben Sie nun unter „**Beschreibung**“ ein, was auf dieser Website zu

finden ist, z.B. eben die „Kinderkanal-Webseite“ und geben Sie unter „**Link zum Angebot**“ die genaue Web-Adresse des Kinderkanals an. Die Beschreibung und der „**Link zum Angebot**“ werden dann wichtig, wenn Ihr Kind z.B. tatsächlich mal eine Seite aufruft, die Sie nicht erlaubt haben. Statt einer Fehlermeldung erscheint dann nämlich eine HTML-Seite im Browser, die alle hier in der Whitelist eingegebenen Webseiten inklusive Beschreibung auflistet. So kann Ihr Kind direkt wieder auf die Seiten zugreifen, die ihm erlaubt sind. Wenn alle Eingaben erfolgt sind, klicken Sie auf „**Hinzufügen**“ und die Whitelist wird um diese Angaben ergänzt.

■ *Der Filter sucht Segmente im Domainnamen. Je nach Angabe im Filter können sich die Ergebnisse also voneinander unterscheiden. Weitere oder engere Einschränkungen sind hier je nach Website hilfreich.*



■ Internetnutzungszeit überwachen

Hier können Sie festlegen, wie lange und zu welchen Zeiten der gewählte Benutzer auf das Internet zugreifen darf. Setzen Sie dazu das Häkchen bei „**Internetnutzungszeit überwachen**“. Nun können Sie festlegen, wie lange der Benutzer im Monat insgesamt ins Internet darf, wie lange pro Woche und wie viele Stunden zu bestimmten Wochentagen. So können z.B. die Wochenenden für schulpflichtige Kinder anders gehandhabt werden, als die Werktage.

Internetnutzungszeit

Wählen Sie hier, wie lange und zu welchen Zeiten der gewählte Benutzer auf das Internet zugreifen darf.
Hinweis: Mit "Zeiten sperren..." können Sie bestimmte Zeiten generell verbieten.

☒ Internetnutzungszeit überwachen (tatsächliche Internet-Aktivität)

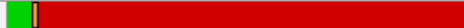
Woche  **02/21:30** Tage/hh:mm

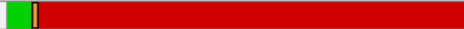
Monat  **01/21:00** hh:mm

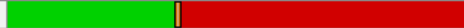
Montag  **01:30** hh:mm

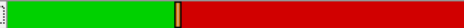
Dienstag  **01:30** hh:mm

Mittwoch  **01:30** hh:mm

Donnerstag  **01:30** hh:mm

Freitag  **01:30** hh:mm

Samstag  **09:00** hh:mm

Sonntag  **09:00** hh:mm

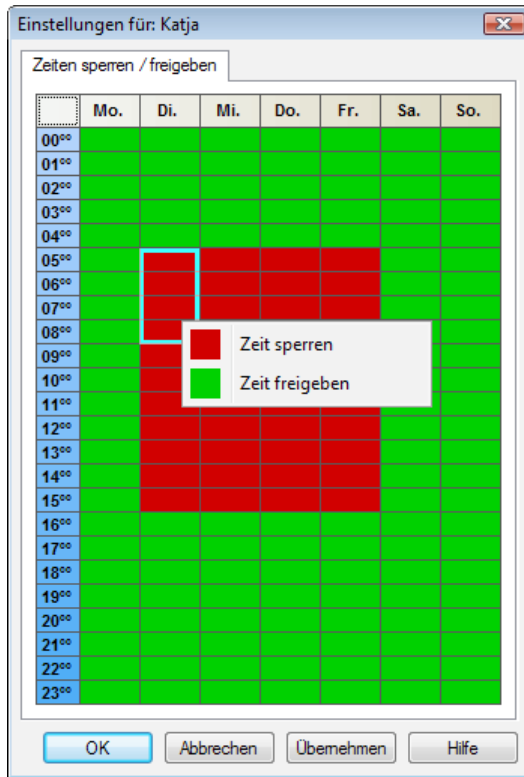
Sie können die entsprechenden **Zeiträume** dazu einfach unter „**Tage/hh:mm**“ eingeben, wobei z.B. die Angabe „04/20:05“ eine Internetnutzungszeit von 4 Tagen, 20 Stunden und 5 Minuten ergäbe.

■ *Im Zusammenspiel der Angaben zur Internetnutzung zählt immer der jeweils kleinste Wert. Wenn Sie also für den Monat eine zeitliche Beschränkung von vier Tagen festlegen, in der Woche aber z.B. fünf Tage erlauben, deckelt die Software die Internetnutzung für den Benutzer automatisch auf vier Tage.*

Wenn der jeweilige Benutzer versucht, über das erlaubte Zeitkontingent hinaus auf das Internet zuzugreifen, erscheint im Browser ein Info-Bildschirm, der ihn darüber informiert, dass er sein Zeitkontingent überschritten hat.

Zeiten sperren

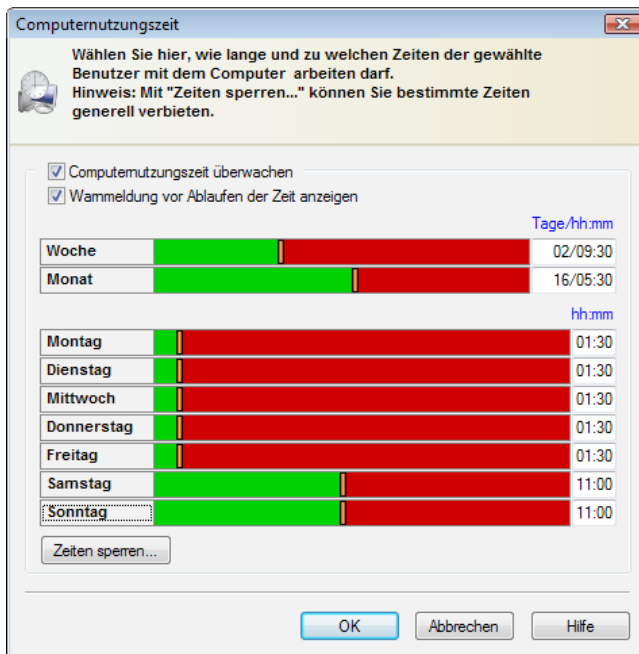
Über den Button „**Zeiten sperren**“ können Sie ein Dialogfeld aufrufen, in dem Sie - zusätzlich zur mengenmäßigen Eingrenzung der Internetnutzung - spezielle Zeiträume in der Woche kategorisch sperren können. Gespernte Zeiträume sind dabei rot dargestellt, freigegebene Zeiträume in grün.



Um einen **Zeitraum** freizugeben oder zu sperren, markieren Sie diesen einfach mit der Maus. Dann erscheint neben dem Mauszeiger ein Kontextmenü, in dem Sie zwei Möglichkeiten haben „**Zeit freigeben**“ und „**Zeit sperren**“. Wenn der jeweilige Benutzer versucht, während der gesperrten Zeiten auf das Internet zuzugreifen, erscheint im Browser ein Info-Bildschirm, der ihn darüber informiert, dass er zu diesem Zeitpunkt keinen Zugriff auf das Internet hat.

■ Computernutzungszeit überwachen

Hier können Sie festlegen, wie lange und zu welchen Zeiten der gewählte Benutzer auf das Internet zugreifen darf. Setzen Sie dazu das Häkchen bei „**Computernutzungszeit überwachen**“. Nun können Sie festlegen, wie lange der **Benutzer** im Monat insgesamt den Computer nutzen darf, wie lange pro Woche und wie viele Stunden zu bestimmten Wochentagen. So können z.B. die Wochenenden für schulpflichtige Kinder anders gehandhabt werden, als die Werktage.



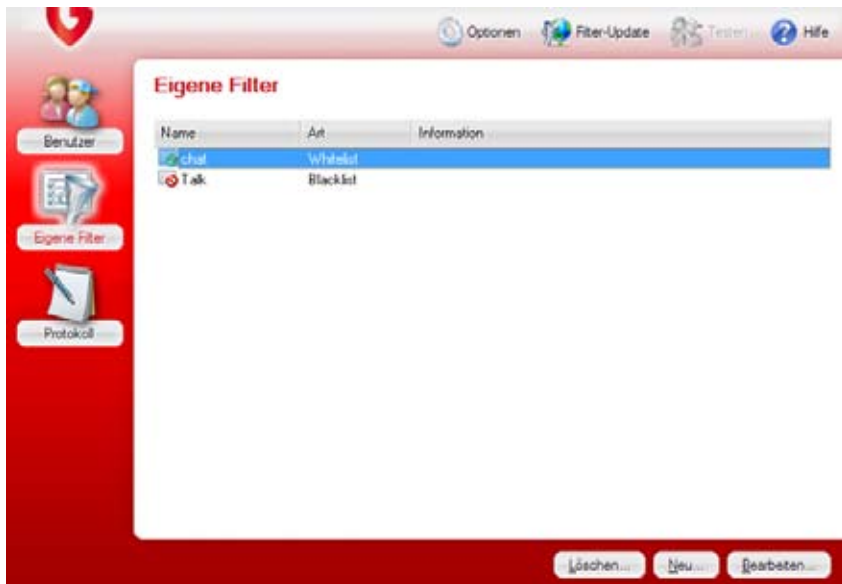
Sie können die entsprechenden **Zeiträume** dazu einfach unter „**Tage/hh:mm**“ eingeben, wobei z.B. die Angabe „04/20:05“ eine Computernutzungszeit von 4 Tagen, 20 Stunden und 5 Minuten ergäbe. Über den Button „**Warnmeldung vor Ablauf der Zeit anzeigen**“ können Sie einen Benutzer kurz bevor der Computer automatisch heruntergefahren wird, informieren, damit dieser noch seine Daten sichern kann. Wird der Computer ohne Warnmeldung heruntergefahren, kann es sonst zu **Datenverlusten** führen.

■ *Im Zusammenspiel der Angaben zur Computernutzung zählt immer der jeweils kleinste Wert. Wenn Sie also für den Monat eine zeitliche Beschränkung von vier Tagen festlegen, in der Woche aber z.B. fünf Tage erlauben, deckelt die Software die Computernutzung für den Benutzer automatisch auf vier Tage.*

Über den Button „**Zeiten sperren**“ können Sie ein Dialogfeld aufrufen, in dem Sie - zusätzlich zur mengenmäßigen Eingrenzung der Computernutzung - spezielle Zeiträume in der Woche kategorisch sperren können. Gesperrte Zeiträume sind dabei rot dargestellt, freigegebene Zeiträume in grün. Um einen **Zeitraum** freizugeben oder zu sperren, markieren Sie diesen einfach mit der Maus. Dann erscheint neben dem Mauszeiger ein Kontextmenü, in dem Sie zwei Möglichkeiten haben „**Zeit freigeben**“ und „**Zeit sperren**“. Wenn der jeweilige Benutzer versucht, während der gesperrten Zeiten oder nach Ablauf seines Zeitkontingents den Computer zu nutzen, wird ihm ein Einloggen nicht gestattet.

■ Eigene Filter

Im Eigene Filter-Bereich können Sie Ihre selbst erstellten Whitelists (also erlaubte Inhalte) und Blacklists (also verbotene Inhalte) verändern und auch komplett neue Listen manuell anlegen.



Die folgenden Listentypen unterscheiden sich grundlegend voneinander:

- **Whitelist:** Wenn Sie für einen der oben ausgewählten Benutzer eine „**Whitelist**“ auswählen, kann dieser ausschließlich Webseiten ansehen, die sich auf dieser Whitelist befinden. Im Bereich „**Stammdaten**“ können Sie als Administrator diese Whitelist nach eigenen Wünschen gestalten oder aus vorgegebenen Whitelists die passende Liste für einen Benutzer auswählen. Eine Whitelist eignet sich besonders dafür, jüngeren Kindern einen sehr begrenzten Zugriff aufs Internet zu erlauben, Ihnen also die Möglichkeit zu geben, Websites mit pädagogisch empfehlenswerten Inhalten zu nutzen, aber nichts darüber hinaus.
- **Blacklist:** Mit einer Blacklist können Sie ausgewählte Webseiten für einen Benutzer sperren. Ansonsten besteht für den Benutzer freier Zugang zum Internet. Beachten Sie, dass Sie über diese Funktion zwar spezielle Seiten sperren können, gleichartige Inhalte aber auch auf anderen Webseiten zur Verfügung stehen können. Eine Blacklist von Internet-Adressen ist in dieser Hinsicht nie ein vollkommener Schutz vor unerwünschten Inhalten.

- Sie können nicht gleichzeitig eine Whitelist zusammen mit einer Blacklist betreiben, da eine Whitelist an sich schon größtmögliche Zugangsbeschränkungen ermöglicht.

Folgende Buttons ermöglichen Ihnen die Bearbeitung der Ausschlusslisten:

- **Löschen:** Über die Löschen-Funktion können Sie mit der Maus ausgewählte Listen einfach löschen.
- **Neu:** Hiermit können Sie eine komplett neue Blacklist oder Whitelist anlegen. Die Vorgehensweise ist dabei dieselbe, wie Sie in den Kapitel „**Benutzer > Verbotene Inhalte**“ und „**Benutzer > Erlaubte Inhalte**“ beschrieben wird.
- **Bearbeiten:** Hiermit können Sie eine bestehende Liste inhaltlich verändern.

■ Protokoll

Im Protokoll-Bereich haben Sie als Administrator eine Übersicht über sämtliche Versuche von anderen Benutzern, geblockte Inhalte aufzurufen. Oben können Sie dazu aus der Liste den Benutzer auswählen, dessen Protokoll Sie sich anzeigen lassen möchten.

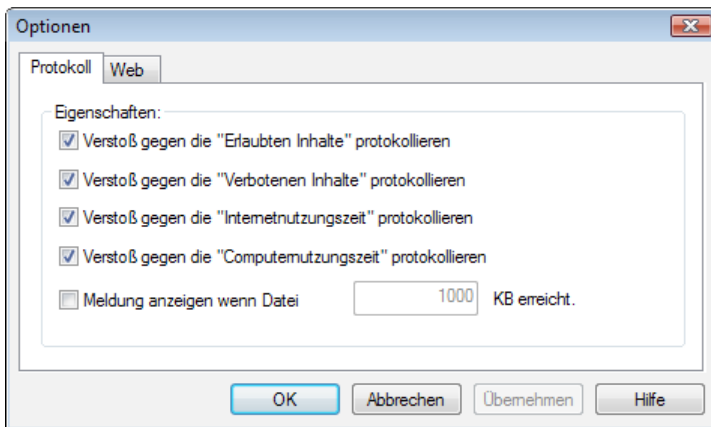


- Sie können diese Protokolle über den Button „Protokolle löschen“ natürlich auch löschen.

■ Optionen

Im Optionen-Bereich können Sie grundlegende Einstellungen der Software verändern. Klicken Sie dazu einfach die Registerkarte mit den jeweiligen Einstellungsoptionen an.

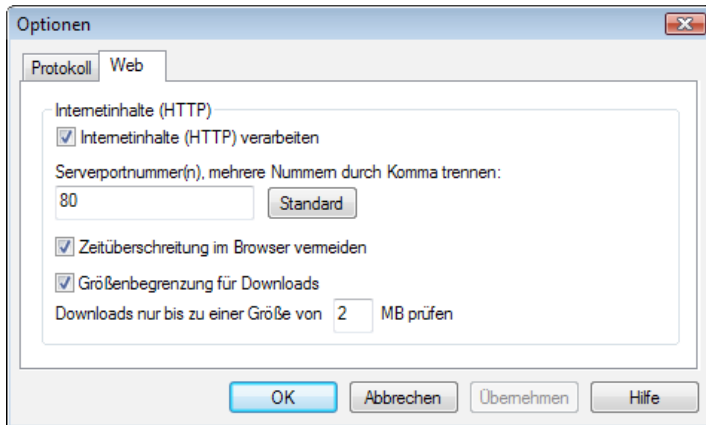
Hier können Sie grundlegende Einstellungen für die Informationen im Protokoll-Bereich verändern. So können Sie festlegen, ob Verstöße gegen erlaubte und/oder verbotene Inhalte protokolliert werden sollen oder nicht. Wenn die Inhalte protokolliert werden, können Sie die Protokolle der unterschiedlichen Benutzer im Protokoll-Bereich einsehen.



■ *Da Protokolldateien bei regelmäßiger Nutzung sehr groß werden, können Sie sich von der Kindersicherung unter „Meldung anzeigen wenn...“ daran erinnern lassen, dass die Protokolldatei eine gewisse Größe überschritten hat und diese dann im Protokolle-Bereich unter „Protokolle löschen“ von Hand löschen.*

■ Web

In den Web-Optionen können Sie bestimmen, dass sämtliche **HTTP-Webinhalte** schon beim Browsen auf relevante Inhalte für Kindersicherung und Webfilter überprüft werden. Unerwünschte Webinhalte werden dann gar nicht erst ausgeführt und die entsprechenden Seiten nicht angezeigt. Setzen Sie hierzu bitte das Häkchen bei „**Internetinhalte (HTTP) verarbeiten**“. Wenn Sie dieses Häkchen nicht setzen, sind Webfilter, Spurenlöscher und Kindersicherung nicht aktiv.



Da der Webfilter die Web-Inhalte vor Ihrer Darstellung im Internet Browser bearbeitet und dafür je nach Datenaufkommen eine gewisse Zeit benötigt, kann es vorkommen, dass eine Fehlermeldung im Internet Browser erscheint, weil dieser nicht sofort die Daten zugestellt bekommt, da diese ja überprüft werden. Mit Aktivieren des Häkchenfeldes „**Zeitüberschreitung im Browser vermeiden**“ wird eine solche **Fehlermeldung** unterdrückt und sobald sämtliche Browserdaten überprüft wurden, werden diese dann ganz normal an den Internetbrowser überreicht.

Mit der „**Größenbegrenzung für Downloads**“ können Sie die HTTP-Überprüfung für zu große Webinhalte unterbrechen. Die Inhalte werden dann vom AntiVirus-Virenwächter überprüft, sobald etwaige Schadroutinen aktiv werden. Der Vorteil bei dieser Größenbegrenzung liegt darin, dass es beim Surfen im Web nicht zu Verzögerungen durch die Virenkontrolle kommt.

■ *Inhalte, die wegen Ihrer Größe nicht VOR Ihrer Anzeige im Browser auf Viren und Schadprogramme überprüft werden, werden vom Wächter natürlich spätestens dann erkannt und geblockt, wenn sie Schadroutinen ausführen möchten.*

Tuner

■ Bedienung des Tuners

Mit dem Tuner können Sie ihr Betriebssystem bequem und unkompliziert optimieren. Von der automatischen Erinnerung an Windows Updates über eine regelmäßige zeitgesteuerte Defragmentierung bis hin zur regelmäßigen Entfernung von überflüssigen Registry-Einträgen und temporären Dateien haben Sie mit dem Tuner ein Tool an der Hand, welches Ihr Windows deutlich schneller und übersichtlicher macht.



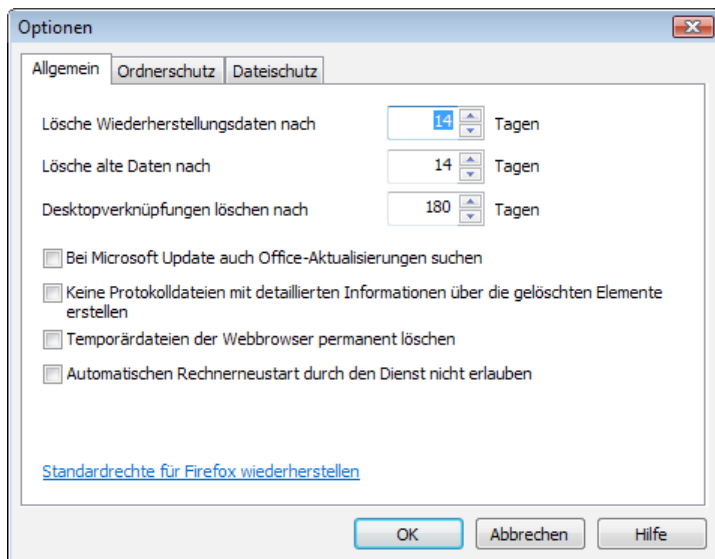
Auf der linken Seite der Programmoberfläche steht Ihnen dazu ein Auswahlbereich zur Verfügung, mit dem Sie die jeweiligen Programmbereiche der Software aufrufen können. Diese werden in den folgenden Kapiteln ausführlich erläutert. Außerdem finden Sie in der oberen Menüleiste der Programmoberfläche übergreifende Funktionen und Einstellungsmöglichkeiten.

■ Optionen

Im Optionen-Bereich können Sie grundlegende Einstellungen der Software verändern. Klicken Sie dazu einfach die Registerkarte mit den jeweiligen Einstellungsoptionen an.

■ Allgemein

Hier können Sie bestimmen, wann **alte Daten** (z.B. alte TEMP-Ordner), **Wiederherstellungsdaten** (die die Tuner-Software bei Änderungen anlegt) und **Desktopverknüpfungen** (wenn sie eine entsprechende Zahl von Tagen nicht verwendet wurden) gelöscht werden sollen.



Außerdem können Sie hier festlegen, ob der Tuner automatisch im **Internet** neben der Suche nach den aktuellen **Windows-Updates** auch nach **Office-Aktualisierungen** suchen soll oder nicht.

- *Die Suche nach Office-Aktualisierungen funktioniert natürlich nur, wenn Microsoft Office auch auf dem jeweiligen Rechner installiert ist.*

Der Tuner ist so aufgebaut, dass er lückenlose Informationen über durchgeführte Änderungen protokolliert. Wenn Sie eine Protokolldatei mit entsprechenden Informationen darüber, was der Tuner gelöscht hat, als Sicherheitsrisiko ansehen, können Sie die Erstellung eines solchen Lösch-Protokolls unterdrücken, indem Sie das Häkchen bei „**Keine Protokolldateien mit detaillierten Informationen über die gelöschten Elemente erstellen**“ setzen. Im Bereich „**Protokolle**“ werden diese Informationen dann nicht in ausführlicher Form angezeigt.

Mit der Funktion „**Temporärdateien der Webbrowser permanent löschen**“ schließen Sie die Webdateien (z.B. Cookies, temporäre Internetdaten) aus der Wiederherstellungsoption des Tuners aus, d.h. Sie können diese Dateien nicht über den Programmbereich „**Rückgängig**“ wiederherstellen.

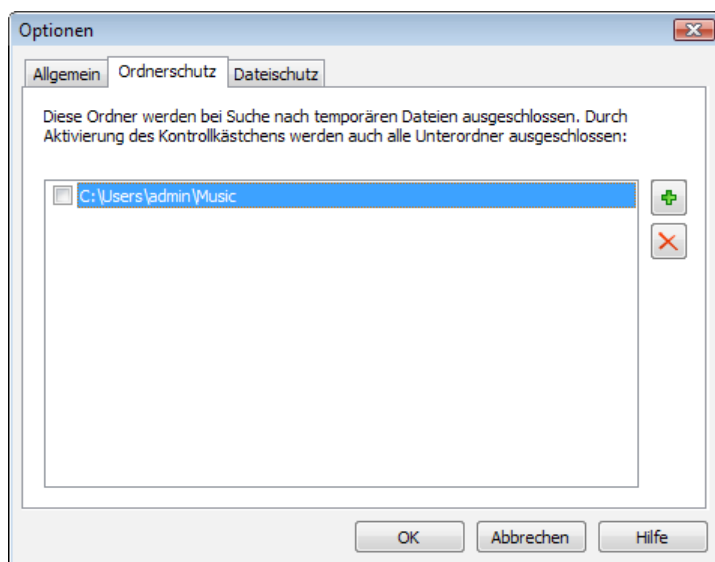
- ☐ *Indem Sie diese Funktion aktivieren, verringern Sie die Menge der Dateien, die der Tuner im Rückgängig-Bereich verwalten muss erheblich. Dies bringt Performance-Vorteile mit sich.*

Mit der Option „**Automatischen Rechnerneustart durch den Dienst nicht erlauben**“ unterbinden Sie einen möglichen Rechnerneustart, den der Tuner bei einem zeitgeteuerten Tuning-Job sonst gegebenenfalls durchführen würde. Da der Tuner einen Rechnerneustart ungefragt nur dann durchführen würde, wenn kein Benutzer angemeldet ist, ist es sicherlich in den meisten Fällen ratsam, diese Option nicht zu aktivieren. Falls Sie den **Firefox-Browser** nutzen, können Sie mit der Funktion „**Standardrechte für Firefox wiederherstellen**“ die Sicherheit des Firefoxbrowsers weiter erhöhen.

- ☐ *Der Firefox-Browser startet beim Umschalten auf Standardrechte von da an immer mit einer Sicherheitsabfrage, außerdem sind Speicheraktionen des Browsers nur noch in Ordnern mit derselben Sicherheitsstufe möglich, d.h. Sie können Daten aus dem Internet nur in einem vorkonfigurierten Downloadordner oder auf dem Desktop speichern.*

■ Ordnerschutz

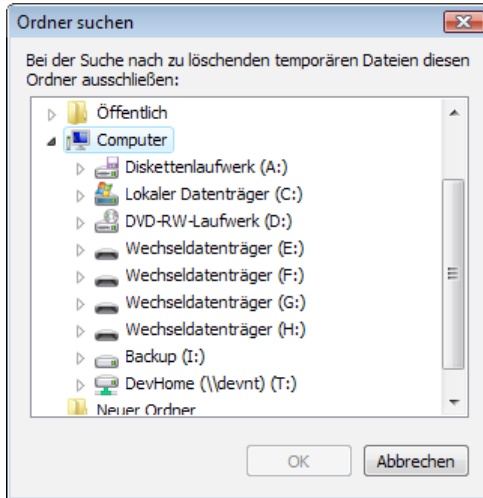
Über die Karteikarte „**Ordnerschutz**“ können Sie bestimmte Ordner (z.B. auch ihre Windows-Partition) von der automatischen Löschung alter Dateien ausnehmen. Klicken Sie dazu einfach auf das **Hinzufügen**-Symbol und wählen dann den entsprechenden Ordner bzw. das gewünschte Laufwerk aus.





Um ein **Ausnahmeverzeichnis** wieder freizugeben, wählen Sie es bitte in dem Bereich „**Temporäre Dateien**“ aus und klicken dann auf den **Löschen**-Button.

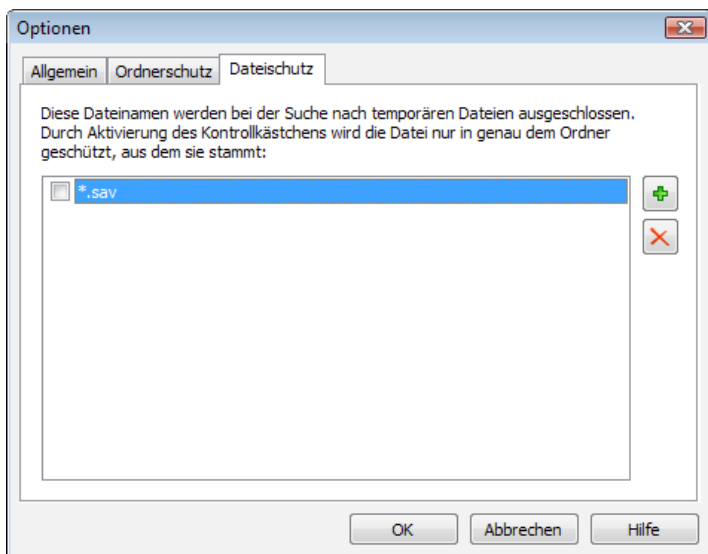
- Zur Suche von temporären Dateien stützt sich die Tuner-Software auf Datei-Endungen. Folgende Datei-Arten werden dabei als temporäre Dateien definiert: `file*.chk`, `*.tmp`, `*.temp`, `*.gid`, `*.bak`, `*.sik` und `*.old`.



- Sie definieren hier explizit einzelne Verzeichnisse als Ausnahme. Wenn Sie also z.B. „C:“ als Ausnahme definieren, werden ausschließlich die Dateien in der obersten Verzeichnisebene von C:\ (dem Rootverzeichnis) geschützt. Temporäre Dateien in den Unterordnern dieses Verzeichnisses (z.B.: „C:\Windows“ oder „C:\Daten\Storage“) werden ganz normal nach Temp-Dateien durchsucht und gegebenenfalls bereinigt.

■ Dateischutz

Mit dem **Dateischutz** können Sie bestimmte Dateien vor der Löschung durch den Tuner schützen, z.B. Spielstände von Computerspielen oder ähnliche Dateien mit unüblichen Dateiendungen, die auch als Backup- oder Temp-Dateien interpretiert werden könnten.



Um bestimmte Dateien zu schützen, klicken Sie auf den **Hinzufügen**-Button und geben den entsprechenden Dateinamen ein. Sie können hier auch mit Platzhaltern arbeiten (z.B. „?“ für ein beliebiges Zeichen oder „*“ für eine beliebige Zeichenfolge).

 Die Funktionsweise von Platzhaltern ist folgendermaßen:

- ? Das Fragezeichen-Symbol ist Stellvertreter für einzelne Zeichen.
- * Das Sternchen-Symbol ist Stellvertreter für ganze Zeichenfolgen.

*Um z.B. sämtliche Dateien mit der Dateiendung „.sav“ zu schützen zu lassen, geben Sie also *.*.sav ein. Um z.B. Dateien unterschiedlichen Typs mit einem anfänglich gleichen Dateinamen zu schützen, geben Sie beispielsweise text*.* ein.*

Wählen Sie nun noch den Ordner aus, in dem die Dateien geschützt werden sollen, indem Sie auf den „...“-Button klicken. Wählen Sie hier nun den Speicherort aus, an dem sich die zu schützenden Dateien befinden. Der Tuner schützt nun die entsprechend definierten Dateien nur in diesem Ordner (z.B. Spielstände nur im jeweiligen Spiele-Ordner).

Hilfe

Hier rufen Sie die Online-Hilfe zum Produkt auf.

■ Programmbereiche

■ Status

Im Statusbereich erhalten Sie eine Übersicht über alle maßgeblichen Informationen zum Betrieb der Tuner-Software.



Folgende Informationen stehen Ihnen im Status-Bereich zur Verfügung. Aktivierte Elemente sind dabei grün dargestellt, nicht aktive Elemente grau:

- **Dienststatus:** Der Dienststatus zeigt an, dass die Tuner-Software aktiv ist.
- **Letzte Ausführung:** Hier wird Ihnen angezeigt, wann die letzte Durchlauf der Tuner-Software erfolgte. Dabei werden hier sowohl automatische, als auch manuelle Ausführungen angezeigt. Wenn Sie einen Tuning-Vorgang direkt starten möchten, klicken Sie einfach auf den Eintrag „**Letzte Ausführung**“ oder den Button „**Ausführen**“. Die Software untersucht dann umgehend Ihr System und optimiert Sie gemäß der Konfigurationen, die Sie im Programmbereich „**Konfiguration**“ einstellen können. Während des Tuningvorgangs erscheint ein weiteres Informationsfeld, in dem die momentan durchgeführte Tuningfunktion angezeigt wird. Sobald das Tuning beendet ist, verschwindet diese Anzeige wieder. Während der Ausführung des Tuningvorgangs informiert ein Fortschrittsbalken über den Fortgang der Aktivität. Dieser Fortschrittsbalken ist sowohl im Statusbereich als auch im Konfigurationsbereich sichtbar.

- **Ausgeführte Änderungen:** Hier finden Sie die Anzahl der bisher durch das Tuning durchgeführten Systemänderungen. Durch Doppelklick auf diesen Eintrag können Sie den Änderungszähler wieder zurücksetzen.
- **Zeitplanung:** Wenn Sie im Bereich „**Zeitplan**“ eine automatische zeitgesteuerte Systemprüfung definieren, wird Ihr Computer regelmäßig nach ihren zeitlichen Vorgaben optimiert. Wenn Sie die automatisierten Tuningvorgänge nicht durchführen möchten, können Sie entweder im Bereich „**Zeitplan**“ den jeweiligen Tuning-Job löschen oder deaktivieren oder mit dem Anklicken des Eintrags „**Zeitplanung**“ alle Tuning-Jobs vorübergehend deaktivieren. Der Eintrag wird dann als „**inaktiv**“ angezeigt. Um die automatische Ausführung wieder zu starten, klicken Sie einfach erneut auf den Eintrag.
- **Defragmentierung:** Die Tuner-Software startet bei zeitgesteuerten Tuning-Jobs auch regelmäßig eine Hintergrund-Defragmentierung Ihres Systems. Sollten Sie aus bestimmten Gründen (z.B. Performance-Problemen) die Defragmentierung nicht wünschen, können Sie diese mit einem Klick auf den Eintrag „**Defragmentierung**“ unterbinden bzw. gerade durchgeführte Defragmentierungen unterbrechen. Der Eintrag wird dann als „**inaktiv**“ gekennzeichnet. Durch Anklicken dieses Eintrags können Sie eine Defragmentierung auch direkt starten bzw. eine laufende Defragmentierung abbrechen.
- **Aktives Profil:** Sie haben die Möglichkeit, unterschiedliche Tuning-Profile zu definieren, so können Sie unabhängig voneinander z.B. ein Sicherheits-, Leistungs- oder Datenschutz-tuning durchführen. Wenn Sie keine unterschiedlichen Profile definieren, wird hier das Profil „**[Standard]**“ angezeigt. Individuelle Profile können Sie im Programmbereich „**Konfiguration**“ anlegen.
- **Aktive Tuningfunktion:** Das Feld „**Aktive Tuningfunktion**“ zeigt ihnen während eines Tuning-Vorgangs an, welche Komponente gerade optimiert bzw. überprüft wird. Nach dem Tuningvorgang wird diese Anzeige automatisch wieder ausgeblendet.

■ Konfiguration

Im Konfigurationsbereich können Sie alle Module auswählen, die die Tuner-Software für einen Tuning-Vorgang verwenden soll. Ausgewählte Module werden dabei dann entweder über eine automatische zeitgesteuerte Aktion gestartet (siehe Kapitel „**Zeitplan**“) oder manuell, in dem Sie im Status-Bereich den **Ausführen**-Button anklicken. Um ein Modul zu aktivieren, führen Sie einfach einen Doppelklick mit der Maus darauf aus.

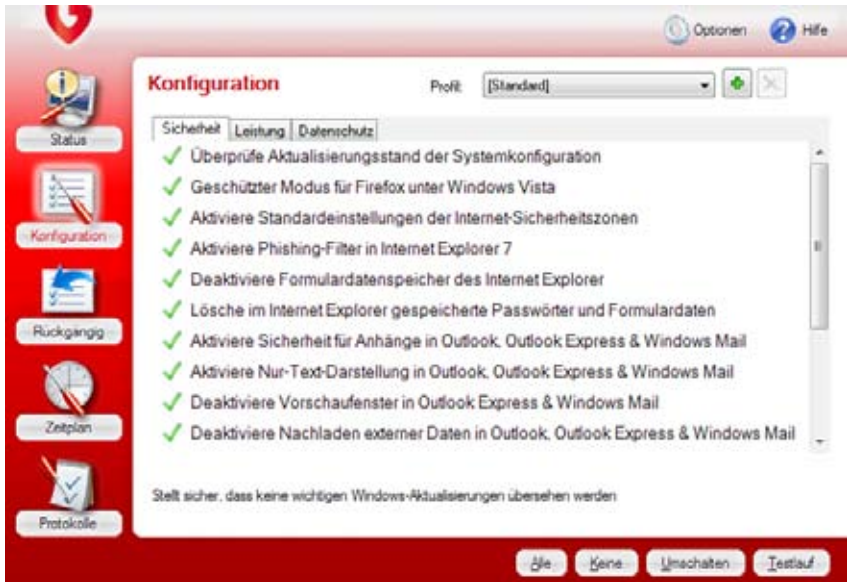


Aktivierte Module werden durch ein grünes Häkchensymbol gekennzeichnet.



Deaktivierte Module werden durch ein rotes Verbotsschild symbolisiert.

Über den **Alle**-Button können Sie alle Module einer speziellen Kategorie (z.B. Sicherheit, Leistung oder Datenschutz) einschalten, über den **Keine**-Button können Sie alle Module ausschalten und über den **Umschalten**-Button können Sie alle aktiven Module ausschalten und alle inaktiven Module anschalten.

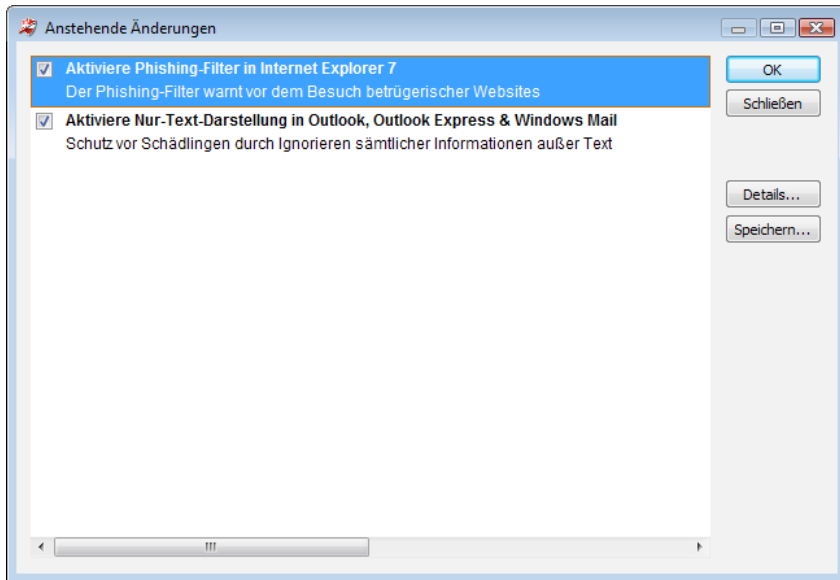


- Um zwischen den einzelnen Kategorien umzuschalten, klicken Sie einfach auf den Karteireiter über der jeweiligen Registerkarte „Sicherheit“, „Leistung“ oder „Datenschutz“.



Über den **Testlauf**-Button haben Sie die Möglichkeit, festzustellen, welche Änderungen der Tuner bei einem Tuning-Vorgang durchführen würde, ohne diese Änderungen tatsächlich durchzuführen. Nach einem Testlauf erscheint ein Bildschirm, in dem die **anstehenden Änderungen** dokumentiert werden. Wenn Sie hier auf „**OK**“ klicken, werden die Änderungen tatsächlich durchgeführt, ein Klick auf den **Schließen**-Button sorgt dagegen dafür, dass keine der im Testlauf vorgeschlagenen Änderungen am System durchgeführt wird.

- Wenn Sie nicht alle vorgeschlagenen Änderungen durchführen möchten, entfernen Sie einfach das Häkchen an der nicht gewünschten Tuning-Option. Wenn Sie nun auf „**OK**“ klicken, ändert die Tuner-Software nur die Elemente, die mit einem Häkchen versehen sind.



Über den **Details**-Button können Sie sich zu dem mit der Maus ausgewählten Änderungsvorschlag ein ausführliches Protokoll anzeigen lassen. Dies können Sie über den **Speichern**-Button auch als Datei im TXT-Format exportieren. Folgende Module stehen Ihnen im Konfigurationsbereich zur Verfügung:

■ Datenschutz

Hier sind die Module zusammengefasst, die sich mit dem Schutz Ihrer Daten befassen. Spuren, die beim Surfen oder der allgemeinen Computernutzung unfreiwillig entstehen und viel über Ihr Nutzerverhalten oder sogar wichtige Daten und Passwörter verraten, werden hier gelöscht:

- **Lösche Verlaufslisten des Windows Explorers:** Der **Windows Explorer** speichert diverse Verlaufslisten (z.B. für Datei- und Computersuche). Diese werden auf Wunsch automatisch gelöscht.
- **Lösche Verlaufsliste zuletzt geöffneter Dokumente:** Hiermit wird die Verlaufsliste der mit Windows geöffneten Dokumente gelöscht. Hierbei handelt es sich um die Liste, die Sie z.B. über „**Start > Dokumente**“ erreichen können.
- **Lösche Verlaufsliste des Windows-Suchassistenten:** Gespeicherte Informationen über frühere **Suchvorgänge** werden mit Hilfe dieses Moduls gelöscht.
- **Lösche Internet Explorer Verlaufsprotokoll:** Die Verlaufsliste der mit dem Internet Explorer besuchten Websites wird gelöscht. Die Verlaufsliste gibt einen

lückenlosen chronologischen Überblick über alle Webseiten, die Sie mit dem Internet Explorer besucht haben.

- **Lösche Internet Explorer Cache:** Die zwischengespeicherten Daten besuchter Websites können viel Festplattenspeicher belegen, außerdem geben Sie einen Überblick über Ihr Surfverhalten. Sie sollten diese Dateien regelmäßig löschen.
- **Lösche Internet Explorer Cookies:** Cookies enthalten personalisierte Daten von besuchten Internetseiten. Einerseits kann ein Anbieter von Websites so Ihre Surfgewohnheiten bis zu einem gewissen Grad nachverfolgen, aber gerade auf Ihrem Computer selbst kann eine Einsichtnahme in die Cookie-Daten sehr viel von Ihrem Surf-Verhalten verraten.
- **Lösche Firefox Verlaufsprotokoll:** Wenn Sie neben dem Internet Explorer auch den Firefox-Browser verwenden, wird Ihr Surfverhalten natürlich auch vom Firefox-Browser dokumentiert. Die Verlaufsliste der mit Firefox besuchten Websites wird mit diesem Modul gelöscht.
- **Lösche Firefox Cache:** Die zwischengespeicherten Daten besuchter Websites können viel Festplattenspeicher belegen.
- **Lösche Firefox Cookies:** Cookies enthalten personalisierte Daten von besuchten Internetseiten. Einerseits kann ein Anbieter von Websites so Ihre Surfgewohnheiten bis zu einem gewissen Grad nachverfolgen, aber gerade auf Ihrem Computer selbst kann eine Einsichtnahme in die Cookie-Daten sehr viel von Ihrem Surf-Verhalten verraten.
- **Lösche Netscape Verlaufsprotokoll:** Wenn Sie neben dem Internet Explorer auch den Netscape-Browser verwenden, wird Ihr Surfverhalten natürlich auch vom Netscape-Browser dokumentiert. Die Verlaufsliste der mit Netscape besuchten Websites wird mit diesem Modul gelöscht.
- **Lösche Netscape Cache:** Die zwischengespeicherten Daten besuchter Websites können viel Festplattenspeicher belegen.
- **Lösche Netscape Cookies:** Cookies enthalten personalisierte Daten von besuchten Internetseiten. Einerseits kann ein Anbieter von Websites so Ihre Surfgewohnheiten bis zu einem gewissen Grad nachverfolgen, aber gerade auf Ihrem Computer selbst kann eine Einsichtnahme in die Cookie-Daten sehr viel von Ihrem Surf-Verhalten verraten.
- **Lösche Opera Verlaufsprotokoll:** Wenn Sie neben dem Internet Explorer auch den Opera-Browser verwenden, wird Ihr Surfverhalten natürlich auch vom Opera-Browser dokumentiert. Die Verlaufsliste der mit Opera besuchten Websites wird mit diesem Modul gelöscht.
- **Lösche Opera Cache:** Die zwischengespeicherten Daten besuchter Websites können viel Festplattenspeicher belegen.
- **Lösche Such-Verlaufsliste des Google Toolbar:** Von verschiedenen Firmen werden sogenannte **Toolbars** als Ergänzung zu Ihrem Desktop oder Internet Browser angeboten. Über diesen Toolbar können Sie bequem und schnell das

Internet nach bestimmten Begriffen durchsuchen. Die Tuner-Software ermöglicht Ihnen, den Verlauf dieser **Internetrecherchen** zu löschen.

- **Lösche Suchen-Verlaufsliste des Windows Live Toolbar:** Beseitigt gespeicherte Suchbegriffe des Windows Live Toolbar.
- **Lösche Such-Verlaufsliste des MSN Toolbar:** Beseitigt gespeicherte Suchbegriffe des MSN Toolbar.
- **Lösche Such-Verlaufsliste des Yahoo! Toolbar:** Beseitigt gespeicherte Suchbegriffe des Yahoo! Toolbar.
- **Deaktiviere Nutzeridentifizierung im Media Player:** Diese Funktion unterdrückt das Versenden der Nutzeridentifikation über den Windows Media Player. Dies dient dem Schutz der Privatsphäre.
- **Unterdrücke Protokollierung von Dateinamen und URLs im Media Player:** Gespeicherte Dateinamen und URLs protokollieren die Nutzung von Medieninhalten und sagen viel über Ihr Nutzungsverhalten aus.

■ Leistung

Temporäre Dateien, z.B. nicht mehr benötigte Sicherheitskopien, Protokolldateien oder Installationsdaten, die nach der Installation nur noch Festplattenplatz belegen, bremsen Ihre Festplatte aus und belegen wertvollen Speicherplatz. Darüber hinaus verlangsamen nicht mehr benötigte Prozesse und Dateiverknüpfungen Ihr System merklich. Mit den hier aufgelisteten Modulen können Sie Ihren Rechner von diesem überflüssigen Ballast befreien und beschleunigen:

- **Defragmentierung aller Festplatten:** Beim Beschreiben und Löschen von Daten auf Datenträgern werden diese Daten zunehmend **fragmentiert**, also eigentlich zusammenhängende Daten auf verschiedenen Bereichen der Festplatte gespeichert. Ein direkter Zugriff auf die Daten wird dadurch verzögert, da der Lesekopf die entsprechenden Informationen an verschiedenen Stellen auf der **Festplatte** auslesen muss. Mit einer regelmäßigen Defragmentierung werden die Daten auf dem Datenträger so sortiert, dass zusammenhängende Segmente auch auf benachbarten Orten auf der Festplatte gespeichert werden. Der Lesekopf muss dann nicht mehr so oft die Position wechseln und der Zugriff auf die Daten beschleunigt sich damit deutlich.
- **Reaktiviere schnellen DMA-Modus für Laufwerke:** Als Folge wiederholter Lesefehler kann der sehr langsame **PIO-Modus** für **Festplatten** und andere Laufwerke (CD-ROM, DVD-ROM) aktiviert worden sein. Im Gegensatz zum **DMA-Modus** ist dieser zwar sicherer, aber auch deutlich langsamer im Datenaustausch mit dem Arbeitsspeicher. Sollte Ihr Computer öfter in den PIO-Modus zurückfallen, kann dies auf einen Hardwarefehler hindeuten.
- **Lösche Dateien im Papierkorb endgültig:** Die im **Papierkorb** aufbewahrten Dateien können beträchtlichen Speicherplatz belegen. Es empfiehlt sich,

den Papierkorb regelmäßig zu leeren. Wenn Sie mit der rechten Maustaste auf das Papierkorb-Symbol auf Ihrem Desktop klicken und im erscheinenden Kontextmenü den Befehl „**Eigenschaften**“ auswählen, können Sie den Papierkorb individuell konfigurieren.

- **Lösche Protokolldateien des G DATA AntiVirus:** Ältere Protokolldateien des G DATA AntiVirus werden über diese Funktion automatisch gelöscht, um Plattenplatz freizugeben.
- **Lösche Protokolldateien des G DATA Tuner:** Ältere Protokolldateien des G DATA Tuners werden gelöscht, um Plattenplatz freizugeben.
- **Lösche ungültige Einträge in OLE/COM-Registrierung:** Dieses Modul entfernt ungültige Registrierungsinformationen für OLE/COM-Komponenten. OLE ist ein von Microsoft entwickeltes Protokoll, das die Zusammenarbeit unterschiedlicher Anwendungen regelt und so die Möglichkeit eröffnet, verschiedene Dokumentarten miteinander zu verbinden (also z.B. Grafiken, Text, Tabellen etc.)
- **Lösche ungültige Applikationsreferenzen:** Hiermit entfernen Sie aus der Registrierungsdatenbank Verweise auf nicht mehr existente ausführbare Dateien
- **Lösche ungültige Shell-Befehle:** Mit dieser Funktion entfernen Sie **DDE-Befehle** (z.B. print, printto, openas...), die nicht existente Dateien referenzieren. DDE (Dynamic Data Exchange) ist eine Protokollsprache für den Datenaustausch zwischen Anwendungsprogrammen.
- **Lösche ungültige Startmenüeinträge: Verknüpfungen** im Startmenü ohne gültiges zugehöriges Ziel (z.B. nach einer unvollständigen Deinstallation) werden hiermit entfernt.
- **Lösche ungültige Datei-Referenzen:** Hiermit entfernen Sie Einträge in der **Liste gemeinsam verwendeter Dateien** (z.B. unter „**C:\Dokumente und Einstellungen\All Users\Gemeinsame Dokumente**“), die auf nicht existente Dateien verweisen.
- **Lösche ungültige Uninstall-Referenzen:** Dieses Modul entfernt Einträge aus der Liste installierter Anwendungen, deren **Deinstallationsfunktion** beschädigt ist.
- **Lösche ungültige Treiberinformationen:** Leere **Treiberinformationsdateien** können Installationsprobleme verursachen. Mit diesem Modul können Sie entsprechende Dateien und Einträge löschen.
- **Lösche ungültige 'Öffnen mit'-Startbefehle:** Hiermit entfernen Sie ungültig gewordene Einträge in der **Öffnen mit**-Auswahlliste. Den Öffnen mit-Dialog erreichen Sie, wenn Sie im Windows Explorer eine beliebige Datei mit der rechten Maustaste anklicken. Im nun erscheinenden Kontext-Menü finden Sie den Befehl „**Öffnen mit**“ über den Sie den jeweiligen Dateityp permanent oder einmalig mit einem Programm Ihrer Wahl verknüpfen können.
- **Lösche ungültige Autostart-Befehle:** Hiermit löschen Sie Verweise auf Autostart-Programme, die sich nicht mehr auf Ihrem Rechner befinden.
- **Lösche ungültige Einträge in Windows-Verlaufflisten:** Auf diese Weise entfernt

ungültige Verweise aus den **Verlaufslisten** von WordPad, Paint und Windows Media Player. Es wird dabei nicht die komplette Verlaufsliste entfernt, sondern nur die Einträge, die z.B. auf Dokumente verweisen, die nicht mehr am angegebenen Speicherort vorliegen.

- **Lösche ungültige Einträge in Office-Verlaufslisten:** Ungültige Einträge in den Verlaufslisten von Microsoft Office-Produkten werden gelöscht. Es wird dabei nicht die komplette Verlaufsliste entfernt, sondern nur die Einträge, die z.B. auf Dokumente verweisen, die nicht mehr am angegebenen Speicherort vorliegen.
- **Lösche ungültige Einträge in Explorer-Verlaufsliste:** Dieses Modul entfernt ungültige Dokument- und Verknüpfungsverweise aus der Verlaufsliste des **Windows Explorer**. Es wird dabei nicht die komplette Verlaufsliste entfernt, sondern nur die Einträge, die z.B. auf Dokumente verweisen, die nicht mehr am angegebenen Speicherort vorliegen.
- **Lösche ungültige Einträge in 'Öffnen Dialog'-Verlaufsliste** Hiermit entfernen Sie ungültige Dokumentverweise aus der Verlaufsliste der gemeinsam genutzten Dateien-Dialoge. Sie erreichen diesen „**Öffnen Dialog**“, in dem Sie in einem Microsoft Office-Produkt den Befehl „**Datei öffnen**“ auswählen. In dem erscheinenden Dialogfeld sehen sie nun rechts z.B. das Symbol für „**Zuletzt verwendete Dokumente**“. Ungültige Einträge in diesem Verlauf werden mit dem beschriebenen Befehl gelöscht.
- **Lösche ungültige Desktop-Verknüpfungen:** Verknüpfungen auf dem Desktop, die z.B. wegen einer unvollständigen Deinstallation auf Objekte verweisen, die nicht mehr auf Ihrer Festplatte vorhanden sind, werden mit diesem Modul entfernt.
- **Lösche ungenutzte Desktop-Verknüpfungen:** Entfernt Verknüpfungen vom Desktop, die seit längerer Zeit nicht benutzt wurden. Über den Bereich „**Optionen > Einstellungen**“ der Tuner-Software können Sie festlegen, nach wie vielen Tagen ungenutzte Desktop-Verknüpfungen gelöscht werden sollen.
- **Lösche ungültige Browser-Hilfsobjekte:** Mit Hilfe dieses Moduls werden fehlerhafte Registrierungen von Internet-Explorer-Hilfsobjekten gelöscht. Browser-Hilfsobjekte sind Addons für den **Internet Explorer**, die Einfluss auf die Darstellung von Websites nehmen. Oft werden Sie über Spyware installiert und für PopUp-Werbung o.ä. verwendet. Wenn ein AntiSpyware-Tool das Ursprungsprogramm entfernt hat, kann es sein, dass Reste der Installation im Internet Explorer verbleiben. Diese werden über dieses Modul gelöscht.
- **Lösche ungültige Browser-Erweiterungen:** Fehlerhafte Registrierungen von Internet-Explorer-Erweiterungen werden mit diesem Modul gelöscht. Diese können verbleiben, wenn eine Browser-Erweiterungen nicht vollständig deinstalliert wurde (z.B. eine Task-Bar).
- **Lösche temporäre Synchronisationsdateien des Windows Media Player:** Bei der Synchronisations-Konvertierung für mobile Geräten fallen große Datenmengen an. Ein regelmäßiges Löschen dieser temporären Zwischenspeicherungen ist deshalb ratsam.

- **Lösche herunter geladene Installationsdaten** Hiermit löschen Sie aus dem Internet geladene Installationsdateien, die nach der Installation der jeweiligen Software in der Regel unnötig sind.
- **Lösche Windows Hotfix Sicherungsdateien:** Sicherungsdateien zur Deinstallation von **Windows-Updates** belegen Festplattenspeicher. Generell können diese gelöscht werden, wenn das Windows-Update an sich problemlos funktioniert.
- **Lösche 'Datei öffnen'-Verlaufsliste der Office-Anwendungen:** Die Verlaufsliste des ‚Datei öffnen‘-Dialogs von **Microsoft Office** wird gelöscht
- **Lösche 'Datei öffnen'-Verlaufsliste der Microsoft Imaging-Anwendungen:** Die Verlaufsliste des ‚Datei öffnen‘-Dialogs von **Microsoft PictureIt!/Digital Image Pro** wird gelöscht
- **Lösche angepasste Reihenfolge der Einträge im Startmenü:** Die angepasste Reihenfolge im Startmenü wird gelöscht; Einträge werden alphabetisch sortiert angezeigt.
- **Lösche Ordner mit temporären Dateien:** Vergessene temporäre Dateien können beträchtlichen Speicher belegen und auf diese Weise Probleme verursachen. Mit der Tuner-Software können Sie diese temporären Dateien automatisch löschen.
- **Lösche temporäre Dateien auf allen Festplatten:** In allen Ordnern der installierten **Festplatten** werden typische temporäre Dateien gesucht und gelöscht. Zur Suche von temporären Dateien stützt sich die Tuner-Software auf Datei-Endungen. Folgende Datei-Arten werden dabei als temporäre Dateien definiert: file*.chk, *.tmp, *.temp, *.gid, *.log, *.bak, *.sik und *.old. Sie können im Bereich „**Optionen**“ bestimmte Ordner oder Verzeichnisse auch vom Löschen der temporären Verzeichnisse ausnehmen.
- **Lösche Protokolldateien der Fehlerberichterstattung:** Gesicherte Protokolldateien der Windows-Fehlerberichterstattung belegen unnötig Festplattenspeicher. Mit diesem Modul können Sie gelöscht werden.
- **Lösche Thumbnail-Dateien von Google Picasa:** Mit diesem Modul können Sie von der **Bildverwaltungssoftware Picasa** zwischengespeicherte **Miniaturansichten** löschen. Sie löschen mit dieser Funktion natürlich nicht die Originalbilder! Die Miniaturansichten erstellt Picasa bei Bedarf automatisch neu.
- **Lösche Cache-Dateien von Google Earth:** Mit dieser Funktion löschen Sie zwischengespeicherte Dateien von Google Earth, die teilweise erheblichen Speicherplatz benötigen. Sie löschen mit dieser Funktion natürlich ausschließlich zwischengespeicherte Arbeitsdateien. Von Ihnen abgespeicherte Daten, wie z.B. Adressen oder Points of Interest werden nicht gelöscht.
- **Lösche Sicherungen alter Installationsdateien von Apple iTunes:** iTunes belegt durch Installationsdateien sämtlicher historischer Versionen viel Plattenplatz. Diesen können Sie mit dieser Funktion automatisch freigeben.

- **Lösche ungültige ActiveSync-Profildaten:** Um z.B. einen **PocketPC** mit dem Desktop-Rechner zu verbinden, wird die **ActiveSync-Software** verwendet. Ungültige Profildaten können die Einrichtung einer neuen Partnerschaft verhindern.
- **Lösche ungültige ActiveSync-Installationsprogramme:** Um z.B. einen **PocketPC** mit dem Desktop-Rechner zu verbinden, wird die **ActiveSync-Software** verwendet. Ungültige Installationsprogramme können die Einrichtung einer neuen Partnerschaft verhindern.

■ Sicherheit

Diverse Funktionen, die automatisch Daten aus dem Internet nachladen, haben lediglich für den Anbieter und nicht für Sie sinnvolle Aspekte. Oftmals wird über solche Funktionen auch Schadsoftware Tür und Tor geöffnet. Mit diesen Modulen schützen Sie Ihr System und halten es auf dem neuesten Stand:

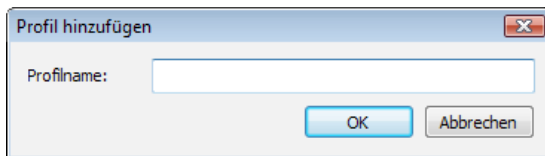
- **Überprüfe Aktualisierungsstand der Systemkonfiguration:** Es gibt in Windows eine Option, automatisch neue **Windows-Updates** aus dem Internet zu laden und zu installieren. Sollte diese Funktion jedoch ausgeschaltet sein, können wichtige sicherheitsrelevante **Updates** möglicherweise übersehen werden. Die Tuner-Software überprüft deshalb regelmäßig, ob neue Windows-Updates im Internet bereit liegen.
- **Reduziere Integritätsstufe für Firefox unter Vista:** Eine reduzierte Integritätsstufe schützt vor potentiellen Sicherheitslücken des Browsers.
- **Aktiviere Standardeinstellungen der Internet-Sicherheitszonen:** Zu schädliche Zoneneinstellungen können Schädlingen das Eindringen in den Rechner erleichtern.
- **Aktiviere Phishing-Filter in Internet Explorer 7:** Der im IE7 integrierte Phishing-Filter warnt vor dem Besuch betrügerischer Websites und sollte möglichst eingeschaltet sein.
- **Deaktiviere Formulare Datenspeicher des Internet Explorer:** In gespeicherten Formulare Daten können persönliche und vertrauliche Daten enthalten sein. Gerade bei der Nutzung eines Rechners mit mehreren Personen ist es ratsam, den Formulare Datenspeicher zu löschen.
- **Lösche im Internet Explorer gespeicherte Passwörter und Formulare Daten:** Alle im Internet Explorer gespeicherten Formulare Daten und Passwörter werden gelöscht. Gerade, wenn Ihr Computer von mehreren Personen genutzt wird, ist es ratsam, das automatische Merken von Passwörtern und Formulare Daten im Internet Explorer zu unterbinden.
- **Aktiviere Sicherheit für Anhänge in Outlook, Outlook Express & Windows Mail:** Wenn Sie diese Funktion aktivieren, werden unsichere Anhänge an Mails (z.B. ausführbare Dateien, wie z.B. „exe“ oder „bat“) von den Microsoft-Mail-Programmen nicht mehr angezeigt bzw. ausgeführt.

- **Aktiviere Nur-Text-Darstellung in Outlook, Outlook Express & Windows Mail:** Wenn Sie diese Funktion aktivieren, werden auch HTML-Mails mit grafischen Elementen als reine Textmails angezeigt. Das minimiert das Risiko, durch nachladbare Grafikdaten eventuell Schadcode auf den Rechner zu bekommen, außerdem verringert es im Zusammenhang mit Spams die Wahrscheinlichkeit, dass Ihre Mailadresse als „aktiv“ in Spam-Listen erscheint, was die Spam-Belastung weiter erhöhen würde.
- **Deaktiviere Vorschauenfenster in Outlook, Outlook Express & Windows Mail:** Schädlinge können potentiell bereits ohne Anwenderaktion im Vorschauenfenster aktiviert werden. Ein Abschalten der Vorschaufunktion ist deshalb aus sicherheitstechnischer Sicht ratsam.
- **Deaktiviere Nachladen externer Daten in Outlook, Outlook Express & Windows Mail:** Das Nachladen von Grafiken und anderen externen Daten einer Mail kann schädlich sein und Informationen über einen Spam-Zustellerfolg preisgeben.
- **Aktiviere Anzeige versteckter Dateien und Dateierweiterungen:** Generell werden versteckte Dateien vom Windows Explorer nicht angezeigt. Dies hat den Vorteil, dass z.B. temporäre Ablagedateien oder z.B. Informationsdateien für Grafikthumbnails nicht im Dateisystem angezeigt werden, sondern nur die für den Anwender relevanten Daten. Allerdings können sich auch Schadprogramme „verstecken“. Normalerweise zeigt der Windows Explorer auch keine Dateierweiterungen an, sondern beschreibt im Klartext, um was für eine Dateiart es sich handelt. Allerdings gibt es auch Schadprogramme, die sich mit „fälschen“ Dateierweiterungen tarnen.
- **Aktiviere Benutzerkontenschutz unter Windows Vista:** Windows Vista können Sie so konfigurieren, dass alle systemrelevanten Änderungen (z.B. die Installation von Programmen) nur mit einer gesonderten Sicherheitsabfrage und den Administratordaten des Rechners erfolgen. Diese Funktion verhindert die heimliche Installation von Schadsoftware und sollte deshalb eingeschaltet sein.
- **Aktiviere Überprüfung der Sicherheit heruntergeladener Dateien:** Gerade beim Dateidownload aus dem Internet ist erhöhte Wachsamkeit geboten. Eine Überprüfung heruntergeladener Daten auf Schadcode ist empfehlenswert.
- **Aktiviere tägliche Updateüberprüfung des Media Players:** Durch die regelmäßige Aktualisierung der Windows Media Player-Daten werden auch potentielle Sicherheitslücken schnell geschlossen.
- **Deaktiviere die Ausführung von Scripten im Media Player:** Die Abschaltung der Scriptausführung im Windows Media Player schützt vor potentiellen Schädlingen.
- **Deaktiviere automatisches Herunterladen neuer Codecs im Media Player:** Mit dem automatischen Nachladen von Codecs bei nicht unterstützten Medienformaten besteht auch die Gefahr, sich Schadsoftware herunterzuladen.

■ Profil definieren



 Sie haben die Möglichkeit, unterschiedliche Tuning-Profile zu definieren, so können Sie unabhängig voneinander z.B. ein Sicherheits-, Leistungs- oder Datenschutz-tuning durchführen. Wenn Sie keine unterschiedlichen Profile definieren, wird hier das Profil „**[Standard]**“ angezeigt. Um ein neues Profil anzulegen, klicken Sie einfach auf den Button „**Ein Profil hinzufügen**“. Nun öffnet sich ein Fenster, in dem Sie einen Namen (z.B. „Sicherheitstuning“ o.ä.) für das neue Profil eingeben können.



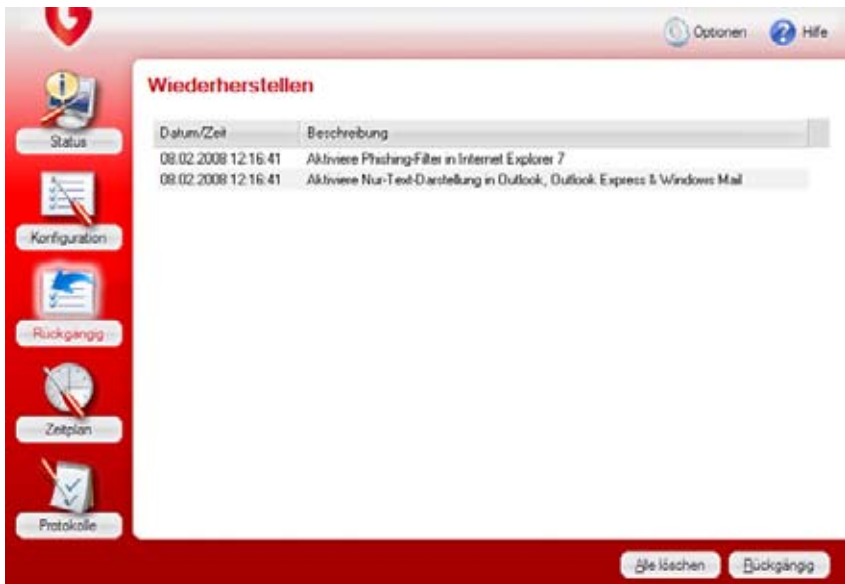
Alle Änderungen, die Sie nun bei der Auswahl der Module vornehmen, werden gespeichert und Sie können so sehr gezielte Tuningläufe durchführen.

 Um ein Profil zu löschen, wählen Sie das Profil aus und klicken dann auf den **Löschen**-Button. Das [Standard]-Profil kann nicht gelöscht werden.

■ Rückgängig

Die Software setzt bei jeder durchgeführten Änderung einen **Wiederherstellungspunkt**. Sollte eine der durchgeführten Tuning-Aktionen zu unerwünschten Ergebnissen geführt haben, können Sie diese so rückgängig machen und den Zustand des Systems vor der jeweiligen Änderung wiederherstellen. Markieren Sie dazu einfach mit der Maus den Bereich, bis zu dem Sie die Wiederherstellung durchführen möchten und klicken dann auf den **Rückgängig**-Button.

 *Sie können hier bewusst nur Bereiche von der aktuellsten Änderung bis maximal zum letzten aufgeführten Wiederherstellungspunkt auswählen. Da Systemoptimierungen und Systembereinigungen aufeinander aufbauen, können Sie z.B. nicht einen in der zeitlichen Abfolge mittig gelegenen Wiederherstellungspunkt alleine auswählen. Eine Wiederherstellung ohne Berücksichtigung der zeitlich darauf folgenden Änderungen würde systembedingt zu Problemen führen.*

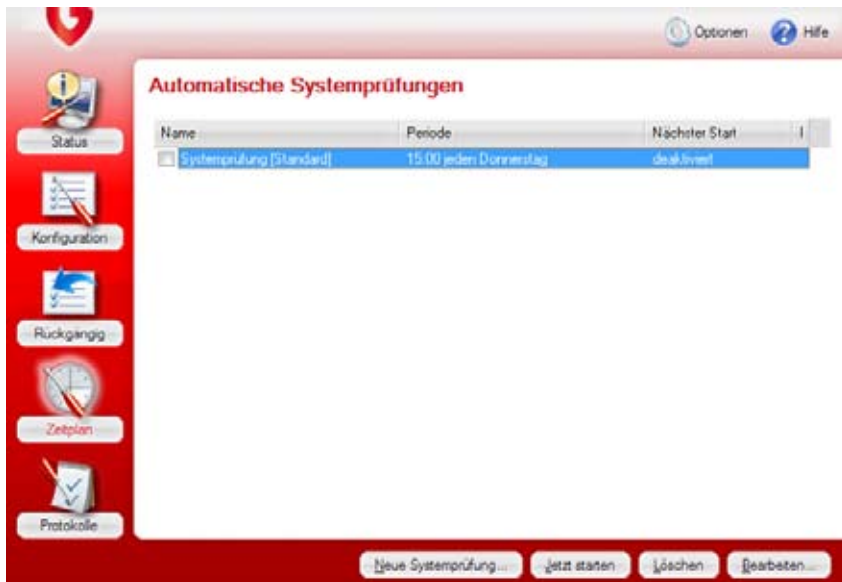


■ Über den Button „**Alle löschen**“ können Sie alle Wiederherstellungspunkte der G DATA-Software löschen. Eine automatische Systemherstellung ist dann nicht mehr möglich. Da die Wiederherstellungsdaten nicht viel Speicherplatz benötigen und Sie im **Optionen**-Bereich die Möglichkeit haben, Wiederherstellungspunkte automatisch nach einer gewissen Zeit zu löschen zu lassen, sollten Sie die auf die manuelle Entfernung der Wiederherstellungspunkte im Regelfall verzichten.

■ Zeitplan

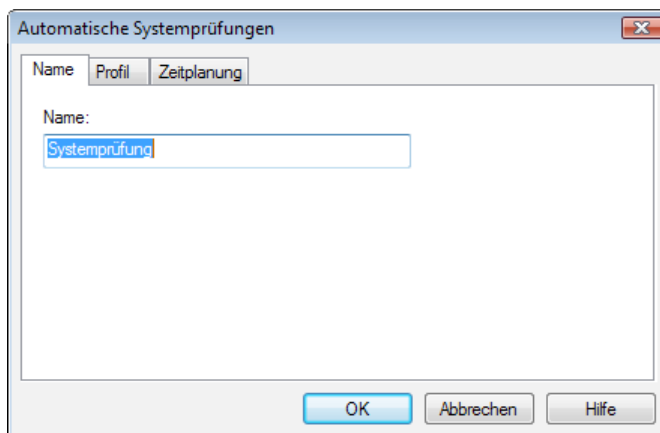
In diesem Bereich können Sie automatische zeitgesteuerte Systemprüfungen definieren. Über den **Bearbeiten**-Button können Sie eine schon bestehende zeitgesteuerte Systemprüfung verändern, über den Button „**Jetzt starten**“ führen Sie ein Tuning unabhängig von den gegebenen zeitlichen Vorgaben sofort durch. Klicken Sie einfach auf den Button „**Neue Systemprüfung**“ und es öffnet sich ein Assistent, in dem Sie alle notwendigen Angaben machen können.

■ Wenn Sie den Auftrag für eine zeitgesteuerte automatische Systemprüfung löschen möchten, klicken Sie den jeweiligen Eintrag einfach mit der rechten Maustaste an und wählen Sie im erscheinenden Kontextmenü den Befehl „**Löschen**“ aus.



■ Name

Geben Sie dazu im Bereich **"Name"** einen aussagekräftigen Namen für die neue Systemprüfung an (z.B. „täglicher Systemcheck“).



■ Profil

Im Bereich können Sie für den jeweiligen Tuning-Job eines der Profile auswählen, die Sie im Bereich **"Konfiguration"** erstellt haben.

■ Zeitplanung

Über die Karteikarte „**Zeitplanung**“ können Sie festlegen, wann und in welchem **Rhythmus** der automatische Tuningjob erfolgen soll. Unter „**Ausführen**“ geben Sie dazu eine Vorgabe vor, die Sie dann mit den Eingaben unter „**Zeitpunkt**“ und „**Wochentage**“ spezifizieren.

■ Unter „Täglich“ können Sie mit Hilfe der Angaben unter „Wochentage“ z.B. bestimmen, dass Ihr Rechner nur an Werktagen das Tuning durchführt oder eben nur an jedem zweiten Tag oder gezielt an Wochenenden, an denen er nicht zur Arbeit genutzt wird. Um unter „Zeitpunkt“ Daten- und Zeiteinträge zu ändern, markieren Sie einfach das Element, das Sie ändern möchten (z.B. Tag, Stunde, Monat, Jahr) mit der Maus und nutzen dann die Pfeiltasten oder die kleinen Pfeilsymbole rechts vom Eingabefeld, um sich im jeweiligen Element chronologisch zu bewegen.

■ Protokolle

Im Protokolle-Bereich finden Sie **Log-Dateien** über alle Tuning-Vorgänge. Hier sehen Sie detailliert, welche Dateien gelöscht oder modifiziert wurden, welche Benutzerkonten und Systembereiche überprüft wurden und welche Einträge in der Registrierungsdatenbank verändert wurden.

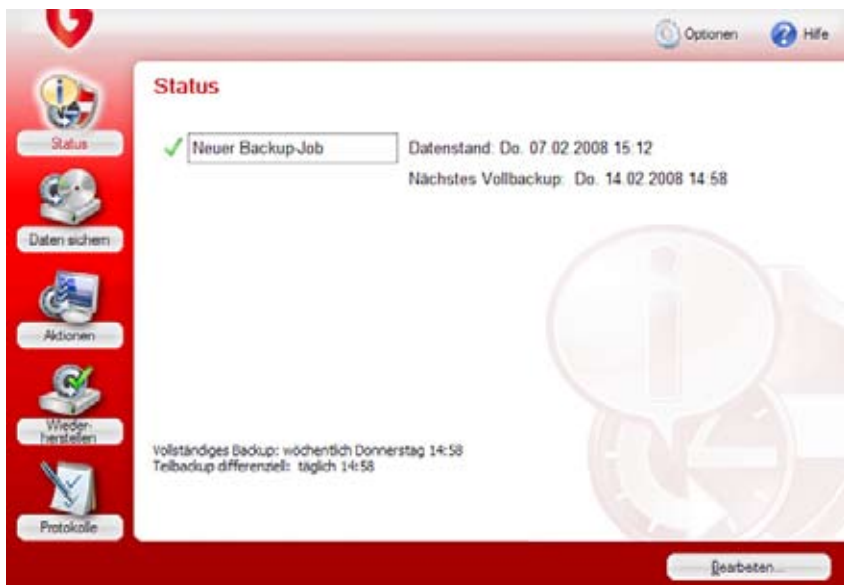


Um sich Details zu einem Protokoll anzuschauen, führen Sie einfach einen Doppelklick auf das gewünschte Protokoll aus oder markieren Sie es und drücken den **Öffnen**-Button. Mit dem **Löschen**-Button können Sie Protokolldateien, die Sie nicht mehr benötigen, manuell löschen.

 *Im Bereich „Konfiguration“ können Sie die Protokolldateien natürlich auch automatisch löschen.*

■ Die Bedienung der Software

Mit fortschreitender Digitalisierung des täglichen Lebens, der Nutzung von Online-Musikdiensten, Digitalkameras und E-Mail-Korrespondenz wird die Sicherung Ihrer persönlichen Daten immer wichtiger. Sei es durch Hardware-Fehler, ein Versehen oder einen Beschädigung durch Viren oder Hacker-Angriffe: Ihre privaten Dokumente sollten regelmäßig gesichert werden. **Backup** übernimmt diese Aufgabe für Sie und schützt so Ihre wichtigen Unterlagen und Dateien, ohne, dass Sie sich ständig Gedanken darum machen müssen. Die Bedienung der Software ist prinzipiell selbsterläuternd und übersichtlich gestaltet. Anhand unterschiedlicher Karteikarten, die Sie über die links angezeigten Symbole anwählen können, wechseln Sie in den jeweiligen Programmbereich und können dort Aktionen durchführen, Voreinstellungen vornehmen oder Vorgänge überprüfen.



Folgende Programmbereiche stehen Ihnen zur Verfügung

- **Status:** Im Status-Bereich erhalten Sie grundlegende Informationen über den aktuellen Stand Ihrer Datensicherungsmaßnahmen.
- **Dateien sichern:** In diesem Bereich können Sie unterschiedliche automatisch ausführbare Datensicherungsjobs erstellen.

- **Aktionen:** Im Aktionen-Bereich können Sie ein Datenbackup manuell starten, sowie zusätzliche FTP- und Brennfunktionen nutzen.
- **Wiederherstellen:** Hier können Sie aus den gespeicherten Backups Dateien wiederherstellen.
- **Protokolle:** Sämtliche Datensicherungs-, Verwaltungs- und Wiederherstellungsvorgänge werden von Backup protokolliert und können eingesehen werden.

Außerdem finden Sie in der oberen Menüleiste der Programmoberfläche übergreifende Funktionen und Einstellungsmöglichkeiten.



Optionen: Hier können Sie grundlegende Einstellungen zum Betrieb von Backup verändern und an individuelle Bedürfnisse anpassen.



Hilfe-Bereich: Hier rufen Sie die Online-Hilfe zum Produkt auf.

■ **Inklusive Online-Speicherplatz (1 GB)**

Mit der Registrierung dieser Software (siehe Kapitel „**ServiceCenter**“) stellt Ihnen G DATA kostenlos 1 GB **Online-Speicherplatz** auf einem **FTP-Server** für Ihre Backups zur Verfügung. Die notwendigen FTP-Daten werden dabei automatisch in die FTP-Maske von Backup übernommen und Sie können Ihre wichtigsten Daten auf diese Weise sicher und bei Bedarf auch passwortgeschützt online verwahren. Sie finden die dazu notwendige **FTP-Zugangsdaten** auf der Rückseite des Bedienungshandbuchs. Wenn Sie die Software online gekauft haben, erhalten Sie die Zugangsdaten in einer gesonderten E-Mail.

■ Bei **Mehrfachlizenzen** steht natürlich für jede Lizenz 1 GB Online-Speicherplatz zur Verfügung, also z.B. bei einer 3-er Lizenz dreimal 1 GB.

■ Solange Sie von G DATA Virensignaturen beziehen, steht Ihnen auch dieser FTP-Speicherplatz zur Verfügung. Nach einer etwaigen Beendigung des Vertrages haben Sie noch 30 Tage Zeit Ihre Daten vom G DATA Backupserver zu entfernen. Danach werden die Daten gelöscht.

■ **Optionen**

Im Optionen-Bereich können Sie grundlegende Einstellungen der Software verändern. Klicken Sie dazu einfach die Registerkarte mit den jeweiligen Einstellungsoptionen an. Sie können diese Optionen entweder individuell für den jeweiligen Backup-Job definieren oder aber global als Voreinstellung für alle Backup-Jobs. Ausführlich werden Ihnen die Optionen im Kapitel „**Ändern eines Backup-Jobs**“ erläutert.

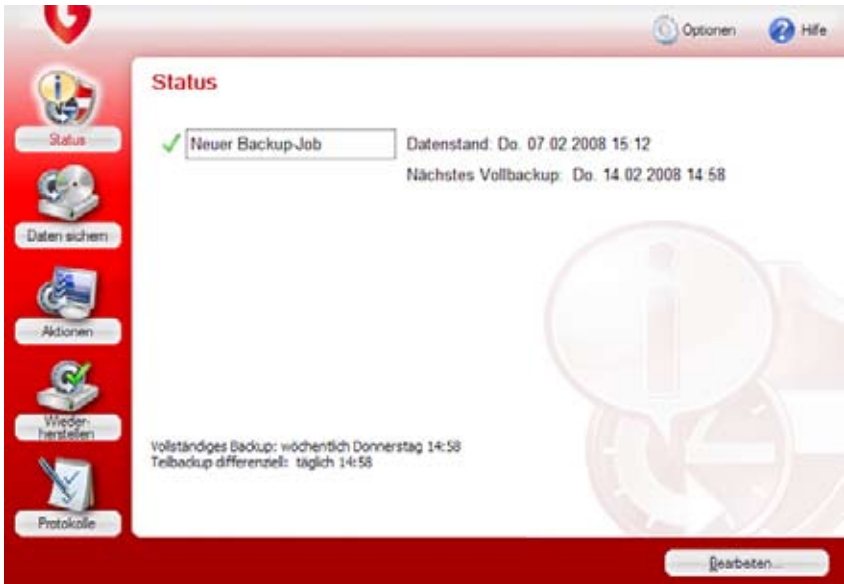
■ Hilfe

Hier rufen Sie die Online-Hilfe zum Produkt auf.

■ Programmbereiche

■ Status

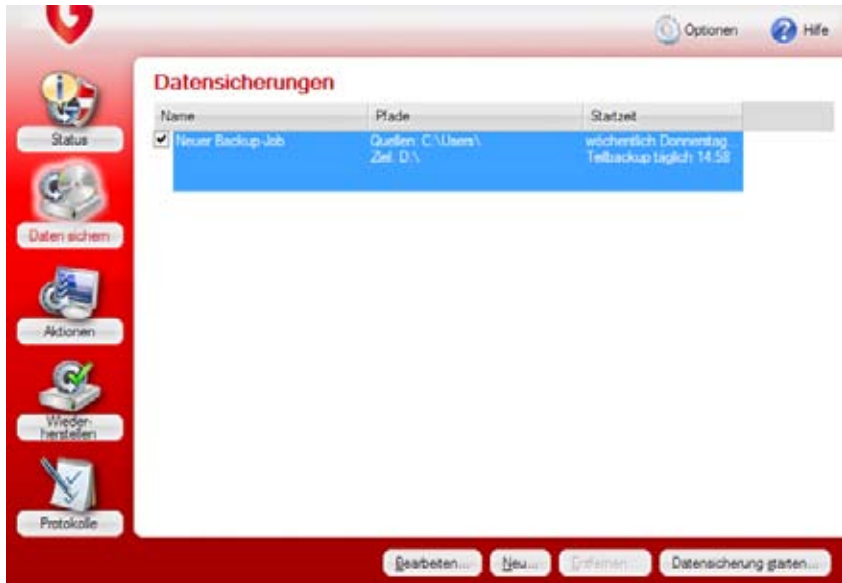
Im Statusbereich erhalten Sie eine Übersicht über den aktuellen Backup-Status. Unter „**Datenstand**“ wird Ihnen gezeigt, von wann das letzte Backup ist und unter „**Nächstes Vollbackup**“ sehen Sie, wann der nächste automatische Backup-Job stattfinden wird. Es ist kein Problem, mehrere voneinander unabhängige Backupvorgänge (z.B. für unterschiedlich wichtige Daten in verschiedenen Abständen) zu verwalten.



Wenn Sie einen Doppelklick auf den gewünschten **Backup-Job** durchführen oder auf den **Bearbeiten**-Button klicken, gelangen Sie in den Programmbereich „**Daten sichern**“ und können dort den jeweiligen Backup-Job verändern, löschen oder neue Backup-Jobs anlegen.

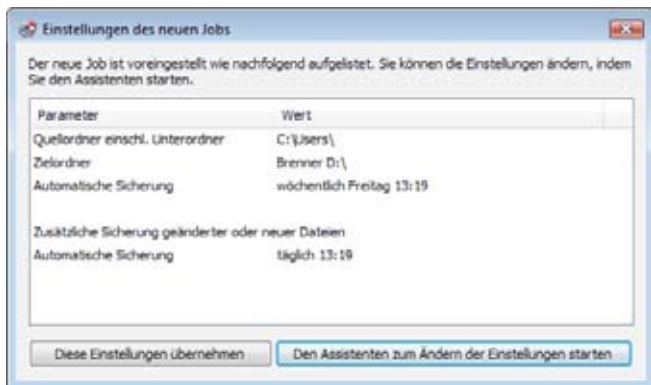
■ Daten sichern

In diesem Programmbereich können Sie assistentengestützt neue Backup-Jobs erstellen oder bestehende **bearbeiten** oder **entfernen**. Über den Button „**Datensicherung starten**“ haben Sie auch die Möglichkeit, unabhängig von den zeitlichen Vorgaben eine Datensicherung sofort durchzuführen.



■ Erstellen eines neuen Backup-Jobs

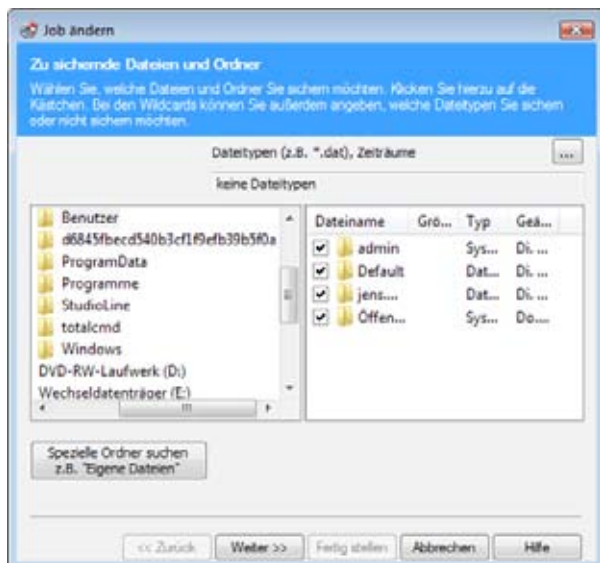
Um einen neuen Backup-Job zu erstellen, klicken Sie einfach auf den **Neu**-Button. Es öffnet sich ein Dialogfenster, welches Ihnen einen standardmäßigen Backup-Job vorschlägt. Bei diesem werden alle persönlichen Dateien aller Benutzer des Computers täglich bei Änderungen und wöchentlich komplett gespeichert. Wenn Sie mit dieser Einstellung zufrieden sind, klicken Sie einfach auf den Button „**Diese Einstellungen übernehmen**“, der Backup-Job wird in die Liste aufgenommen und von nun an werden alle Daten, die unter „**Dokumente und Einstellungen**“ bzw. „**Eigene Dateien**“ anfallen automatisch gespeichert.



Wenn Sie den neuen Backup-Job individuell gestalten möchten, klicken Sie statt dessen auf den Button **„Den Assistenten zum Ändern der Einstellungen starten“**. Nun können Sie die Vorgaben für ein Backup nach Belieben verändern. Ausführliche Informationen hierzu finden Sie in dem Kapitel **„Ändern eines Backup-Jobs“**.

■ Ändern eines Backup-Jobs

Das Ändern eines bestehenden Backup-Jobs wird Ihnen durch einen Assistenten erleichtert, der Sie schrittweise bei den Einstellungen begleitet. Wenn Sie alle notwendigen Änderungen in einem Einstellungsbereich vorgenommen haben, klicken Sie einfach auf **Weiter** und Sie gelangen zum nächsten Assistentenmenü.

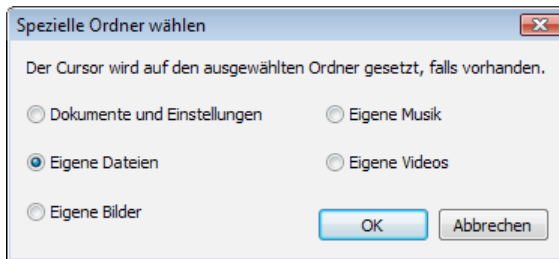


Zu sichernde Dateien und Ordner

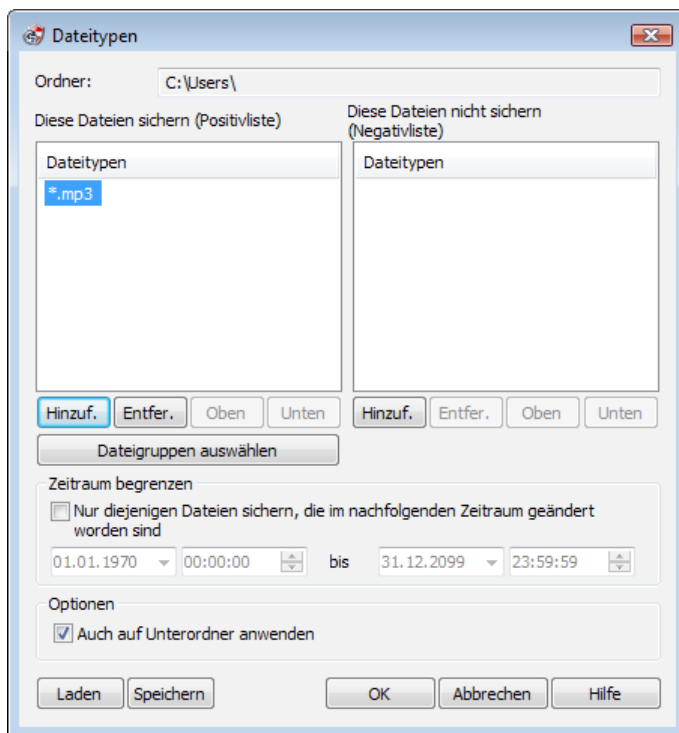
Hier können Sie bestimmen, welche Ordner und Dateien auf Ihrem Computer von **Backup** gespeichert werden sollen. Auf der linken Seite des Fensters finden Sie dazu einen Verzeichnisbaum, in dem Sie z.B. wie im Windows Explorer alle Ordner und Dateien auf Ihrer Festplatte aus- und anwählen können.

- ☒ Wenn Sie ein Häkchen vor den jeweiligen Ordner oder die Datei setzen, berücksichtigt **Backup** den Inhalt dieses Ordners und all seiner Unterordner für die Datensicherung.
- ☐ Wenn Sie das Häkchen entfernen, werden der jeweilige Ordner und seine Dateien/Unterordner nicht mehr gebackuppt.
- ☐ Wenn Sie bestimmte Dateien oder Unterordner vom Backup ausnehmen wollen, können Sie das Häkchen an der jeweiligen Datei bzw. dem jeweiligen Unterordner entfernen. Beim übergeordneten Ordner sehen Sie nun ein quadratisches Symbol, das Sie darauf hinweist, dass in diesem Ordner einige Dateien und Unterordner vom Backup ausgeschlossen wurden.

Wenn Sie sich in der Verzeichnisstruktur von Windows nicht so gut zurechtfinden, können Sie den Button „**Spezielle Ordner suchen**“ anklicken. Es erscheint ein Dialog, in dem Sie festlegen können, ob Sie die Ordner **Dokumente und Einstellungen**, **Eigene Dateien**, **Eigene Bilder**, **Eigene Musik** und/oder **Eigene Videos** suchen. Mit einem Klick auf **OK** springt das Verzeichnisfenster dann an genau diesen Ort und Sie können dann die gewünschten Einstellungen ohne großes Suchen vornehmen.



Wenn Sie nur bestimmte Daten (z.B. nur neue Dateien der letzten 24 Stunden oder nur MP3-Dateien) sichern möchten, klicken Sie einfach auf den Button „**Dateitypen (z.B. *.dat), Zeiträume**“. Hier können Sie dann festlegen, welche Dateitypen für eine Sicherung markiert werden sollen.

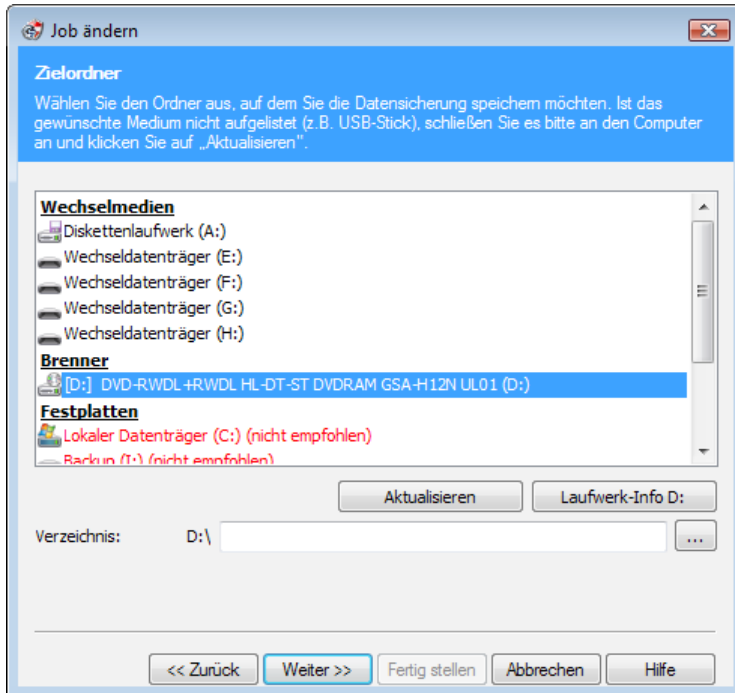


In der **Positivliste** können Sie Dateitypen explizit für eine Speicherung vorschlagen. Klicken Sie dazu auf den **Hinzuf.**-Button und geben den gewünschten Suchstring ein. Das Stern-Symbol fungiert dabei als **Wildcard**, d.h. wenn Sie *.*mp3 eingeben, werden alle Dateien mit der Endung „.mp3“ auf die Positivliste gesetzt. Wenn Sie hier nur „*.*“ eingeben würden, werden ALLE Dateien auf die Positivliste gesetzt. Mit Anklicken des Buttons „**Dateigruppen auswählen**“ können Sie auch gezielt festlegen, dass Musik-, Text- oder z.B. Bilddateien gespeichert werden sollen. Welche Dateierweiterungen zu den jeweiligen Dateigruppen gehören, wird dabei im **Optionen**-Bereich eingestellt. In der **Negativliste** können Sie analog zur Positivliste Dateitypen definieren, die Sie nicht gespeichert wissen möchten (z.B. temp-Dateien). Zusätzlich zur Beschränkung auf einzelne Dateitypen oder -gruppen können Sie auch zeitliche Vorgaben beim Backup definieren. Wenn Sie das Häkchen bei „**Nur diejenigen Dateien sichern, die im nachfolgenden Zeitraum geändert worden sind**“ setzen, können Sie festlegen, dass nur Dateien, die z.B. innerhalb der letzten Woche geändert wurden, beim Backup berücksichtigt werden.

■ Das Häkchen bei „Auch auf Unterordner anwenden“ sollte generell gesetzt bleiben.

Zielordner

Wählen Sie hier den Ordner aus, in dem Sie die Datensicherung abspeichern möchten. Sollte das gewünschte Medium nicht aufgelistet sein (z.B. ein USB-Stick), schließen Sie es bitte an den Computer an und klicken dann auf den **Aktualisieren**-Button. Je nach Ausstattung Ihres Computers haben Sie die Möglichkeit, Backups auf **Wechselmedien** (z.B. **USB-Sticks**, **SD-Karten**, **externen Festplatten**) oder integrierten **Festplatten** durchzuführen.



■ **Achtung:** Bitte achten Sie darauf, dass das Backup nicht auf der gleichen Platte erfolgen sollte, auf der sich auch die Originaldaten befinden. Sollte diese Festplatte nämlich einen Defekt haben, sind Original- und Backup-Daten verloren!

Selbstverständlich können Sie unter „**Brenner**“ Daten auch auf CD oder DVD schreiben, angeschlossene **Netzlaufwerke** verwenden oder die Daten per **FTP** sichern.

Zeitplanung

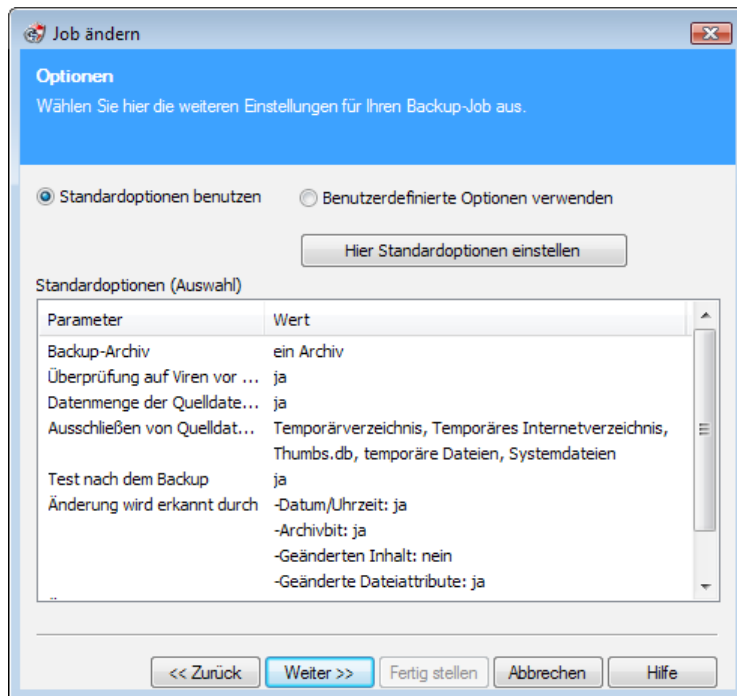
Über diese Karteikarte können Sie festlegen, wann und in welchem Rhythmus das automatische Update erfolgen soll. Unter „**Ausführen**“ geben Sie dazu eine Vorgabe vor, die Sie dann mit den Eingaben unter „**Zeitpunkt**“ und „**Wochentage**“ spezifizieren.

■ Um unter „Zeitpunkt“ Daten- und Zeiteinträge zu ändern, markieren Sie einfach das Element, das Sie ändern möchten (z.B. Tag, Stunde, Monat, Jahr) mit der Maus und nutzen dann die Pfeiltasten oder die kleinen Pfeilsymbole rechts vom Eingabefeld, um sich im jeweiligen Element chronologisch zu bewegen.

Optionen

Hier können Sie bestimmen, ob Ihr Backup-Job auf die Standardoptionen zurückgreifen soll, die Sie im Bereich **„Optionen“** (siehe Kapitel **„Die Bedienung der Software > Optionen“**) erstellt haben oder ob Sie für diesen speziellen Job eigene Optionen vergeben möchten.

- **Standardoptionen benutzen:** Hier werden Sie zu der Karteikarte für Standardoptionen weitergeleitet und können global die Optionen für alle zukünftigen Jobs verändern.
- **Benutzerdefinierte Optionen verwenden:** Hier können Sie für den aktuellen Job ganz individuelle Vorgaben machen.



Folgende Werte können Sie bei den benutzerdefinierten Optionen verändern:

Art des Archivs

Legen Sie hier fest, wie Sie die zu sichernden Dateien archivieren möchten.

- **Dateien 1:1:** Die zu sichernden Dateien werden in das Zielverzeichnis oder die entsprechenden Unterverzeichnisse kopiert. Die erzeugte Archivdatei dient dabei als Inhaltsverzeichnis. Zu sichernde Dateien werden nicht komprimiert. Über das Häkchen bei „**Schreibgeschützte Dateien überschreiben**“ können Sie bestimmen, ob schreibgeschützte Dateien beim Backup an der jeweiligen Position überschrieben werden sollen oder nicht.
- **Dateien komprimiert einzeln:** Die zu sichernden Dateien werden als komprimierte Dateien in das Zielverzeichnis oder in die entsprechenden Unterordner gesichert. Die erzeugte Archivdatei dient dabei als Inhaltsverzeichnis.
- **Ein Archiv:** Alle zu sichernden Dateien werden einschließlich aller Speicherattribute in eine oder bei sehr großen Speichermengen mehrere Archivdateien gespeichert. Archivdateien haben die Dateiendung „.arc“ und können automatisch durch ein **Passwort** geschützt werden.

■ **Achtung:** Eine Speicherung im Format „Dateien 1:1“ kann nicht erfolgen, wenn die Dateien auf dem G DATA FTP-Server gespeichert werden sollen. Speicherungen an diesem Ort können nur einzeln komprimiert oder als Archiv erfolgen, da aus Sicherheitsgründen für den G DATA FTP-Server eine Dateitypbeschränkung besteht. Generell ist eine Speicherung von Daten im 1:1-Format auf Grund von Datenschutzaspekten nicht ratsam.

Passwort

Wenn Sie bei der Art des Archivs die Funktion „**Ein Archiv**“ angewählt haben, können Sie dieses Archiv auch automatisch mit einem Passwort schützen. Auf diese Weise werden Dateien, die Sie z.B. auf einem USB-Stick speichern direkt vor unbefugtem Zugriff geschützt. Beim Wiederherstellen von Dateien wird das Passwort abgefragt.

Virenüberprüfung

Wenn Sie **Backup** in Verbindung mit einem kombinierten Antivirenprogramm verwenden, können Sie Dateien vor dem Sichern auf Virenbefall überprüfen. Wenn Sie dies wünschen, setzen Sie das Häkchen bei „**Vor dem Speichern Dateien auf Viren überprüfen und die infizierten Dateien nicht ins Archiv übernehmen**“. Wenn Sie die Dateien nicht auf Virenbefall überprüfen, erfolgt der Backupvorgang an sich etwas schneller und performance-optimierter. Sie sollten diese Option allerdings nur dann deaktivieren, wenn Ihr System standardmäßig vor Viren und Malware geschützt ist.

Schätzen der Datenmenge

Ein Abschätzen der zu sichernden Datenmenge dient zur verlässlicheren Darstellung der Fortschritts- und Restzeitanzeige. Ein Aktivieren oder Deaktivieren dieser Funktion hat keinen Einfluss auf die erstellten Archive.

Datenkompression

Wenn Sie Ihre Daten komprimiert speichern (siehe „**Art des Archivs**“) können Sie hier festlegen, wie stark die **Kompression** ist. Je höher die **Blockgröße**, desto stärker wird die Kompression, allerdings benötigt diese dann auch länger. Generell sollten die Standardwerte hier beibehalten bleiben.

Zusätzliche Dateien

Sie können beim Speichern der Archive die reinen Ursprungsdaten sichern oder aber Zusatzdateien hinzufügen, die den Komfort des Backup-Systems verbessern. Generell wird empfohlen die zusätzlichen Dateien mitzuspeichern, die Häkchen bei diesen Funktionen also gesetzt zu lassen.

- **Dieses Programm speichern:** Wenn Sie diese Option wählen, wird das Backupprogramm im Archiv mitgespeichert und das Backup kann aus einem Archiv heraus auch wiederhergestellt werden, ohne dass die Backup-Software (z.B. auf einem neuen Rechner) neu installiert werden müsste.

Ausschließen von Quelldateien

Generell sichert **Backup** Dateien auf Basis ihres Dateiformates. Auf Ihrem Computersystem finden sich entsprechende Dateiformate aber auch in Bereichen, die automatisch verwaltet werden und nicht für ein Backup relevant sind, da die jeweiligen Dateien nur temporär gespeichert wurden (z.B. zur Beschleunigung der Seitendarstellung aus dem Internet). Damit **Backup** dies Dateien nicht unnötig mitarchiviert, können Sie diese über das Setzen der jeweiligen Häkchen ausschließen.

- **Temporärverzeichnis mit Dateien:** Wenn diese Option gewählt ist, werden die temporären Ordner (... \Dokumente und Einstellungen\<Benutzer>\Lokale Einstellungen\temp) sowie die dort befindlichen Unterordner und Dateien nicht in die Datensicherung aufgenommen.
- **Temporäres Internetverzeichnis mit Dateien:** Wenn diese Option gewählt ist, werden die Ordner für die Speicherung von Internetseiten (... \Dokumente und Einstellungen\<Benutzer>\Temporary Internet Folders) sowie die dort befindlichen Unterordner und Dateien nicht in die Datensicherung aufgenommen.
- **Thumbs.db:** Wenn diese Option gewählt ist, werden die vom Windows Explorer automatisch erstellten Dateien „thumbs.db“ nicht in die Datensicherung aufgenommen. Diese Dateien dienen z.B. dazu die Miniaturansichten für Slideshows zu verwalten und werden aus den Originalbildern automatisch erzeugt.
- **Temporäre Dateien (Dateiattribut):** Wenn diese Option gewählt ist, werden Dateien mit dem vom System vergebenen Dateiattribut „**temporär**“ nicht in die Datensicherung übernommen.
- **Systemdateien (Dateiattribut):** Wenn diese Option gewählt ist, werden Dateien mit dem vom System vergebenen Dateiattribut „**Systemdatei**“ nicht in die Datensicherung übernommen.

Sicherung auf CD/DVD

Falls Sie Ihre Daten auf CD oder DVD speichern möchten, bietet Ihnen **Backup** folgende Einstellungsmöglichkeiten:

- **Label auf dem Medium:** Sie können die CD/DVD automatisch benennen, so würde Backup für jede Datensicherung ein eindeutiges Label vergeben, welches sich aus Datum, Zeit und laufender Nr. des Datenträgers ermittelt (z.B. 070202_1423_0001). Alternativ können Sie hier auch andere Namen vergeben.
- **Bei erfolgreichem Brennen Zwischendateien löschen:** Es ist empfehlenswert, die temporären Dateien nach dem Brennen einer CD/DVD zu löschen. Bei diesen

Daten handelt es sich natürlich nicht um die zu sichernden Originaldateien, sondern um temporäre Zwischenspeicherungen zur Optimierung des Brennvorgangs. Die Option „**Nicht brennen, nur Zwischendateien erstellen**“ dient dazu Dateien bereitzustellen, die dann für ein nachträgliches Brennen genutzt werden können.

- **Medium nach dem Brennen überprüfen (Verify):** Bei besonders wichtigen Daten kann es sinnvoll sein, zu überprüfen, ob der Brennvorgang auch erfolgreich war. Das Backup dauert dadurch zwar länger, ist aber auch sicherer.
- **Max. Datenmenge je Medium:** Generell stellt Backup bei der Einstellung „automatisch“ selber fest, wie viel Platz auf einem Medium zur Verfügung steht. Wahlweise können Sie den Wert hier aber auch manuell einstellen.

Test nach dem Sichern

Es ist empfehlenswert, nach der Datensicherung auch zu überprüfen, ob die erzeugte Backup-Datei auch mit der Originaldatei übereinstimmt. **Backup** bietet hier verschiedene Möglichkeiten, Original- und Backupdatei miteinander zu vergleichen. Das Häkchen bei „**Nach der Datensicherung testen**“ sollte also in der Regel gesetzt bleiben.

Nach der Datensicherung

Bei manuell gestarteten Backup-Jobs können Sie festlegen, dass der Computer danach heruntergefahren wird. So können Sie z.B. ein großes Backup über Nacht oder zum Dienstschluss anstarten und ihre tägliche Arbeit wird auf diese Weise von dem Backupvorgang nicht betroffen.

Ältere Datensicherungen löschen

Bei regelmäßiger Archivierung Ihrer Daten fallen natürlich große Datenmengen an. Sie können entscheiden, ob Sie alle Backups behalten wollen oder nur die jeweils aktuellsten Backups.

- **nicht löschen:** Wenn Sie ältere Archive nicht automatisch löschen möchten, können Sie diese manuell jederzeit im Programmbereich „**Aktionen**“ löschen.
- **nach einem vollständigen Backup Benutzer fragen:** Sobald alle Daten nach einem vollständigen Backup archiviert wurden, ist ein Behalten der zeitlich davorliegenden Archivdateien nicht unbedingt nötig. Wenn Sie die Option „**Benutzer fragen**“ anwählen, fragt **Backup** Sie nach dem Archivierungsvorgang, wie mit den älteren Archiven verfahren werden soll.
- **nach einem vollständigen Backup automatisch löschen:** Hier können Sie festlegen, dass **Backup** veraltete Archivdateien automatisch löscht. Dabei können Sie bestimmen, wie viele zeitlich vor dem letzten Backup liegende Archivierungen Sie verwahren möchten, z.B. die letzten zwei, drei oder vier Backups.

Deaktivierung

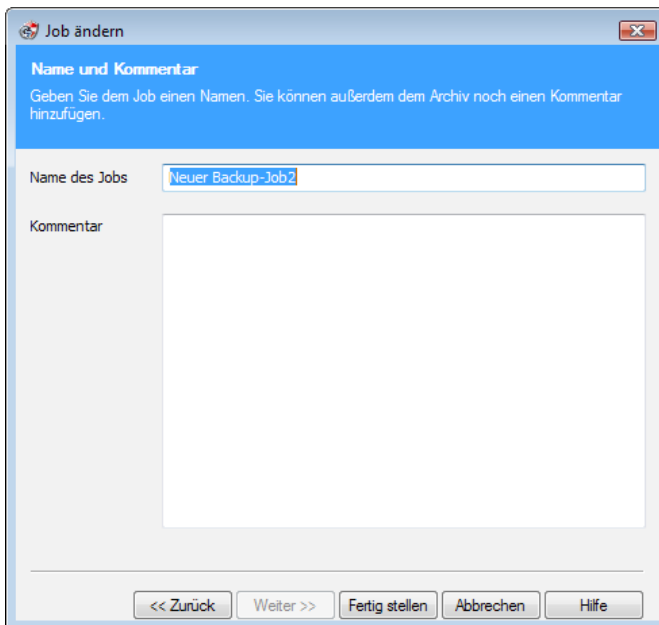
Wenn Sie den benutzerdefinierten Job nicht direkt starten möchten und auch die zeitgesteuerte Ausführung nicht direkt aktivieren möchten, können Sie diese hier deaktivieren.

Thread-Priorität

Eine hohe Priorität beschleunigt die Ausführung des Backups, verlangsamt allerdings auch die Ausführung anderer Programme.

Name und Kommentar

Hier können Sie den Namen des Backup-Jobs verändern. Außerdem können Sie im **Kommentar**-Feld ausführliche Informationen zum erstellten Job eingeben. Gerade dann, wenn viele unterschiedliche Backup-Jobs auf Ihrem Rechner laufen ist dies aus Gründen der Übersichtlichkeit zu empfehlen.



The screenshot shows a Windows-style dialog box titled "Job ändern" (Change Job). The dialog has a blue header bar with the title and a close button. Below the header, the text "Name und Kommentar" (Name and Comment) is displayed, followed by the instruction "Geben Sie dem Job einen Namen. Sie können außerdem dem Archiv noch einen Kommentar hinzufügen." (Give the job a name. You can also add a comment to the archive). There are two input fields: "Name des Jobs" (Job Name) with the text "Neuer Backup-Job2" and "Kommentar" (Comment) which is a large empty text area. At the bottom of the dialog, there are five buttons: "<< Zurück" (Back), "Weiter >>" (Next), "Fertig stellen" (Finish), "Abbrechen" (Cancel), and "Hilfe" (Help).

■ Aktionen

In diesem Bereich können Sie unter anderem Aktionen zur Pflege und Wartung Ihrer Datenbackups vornehmen.

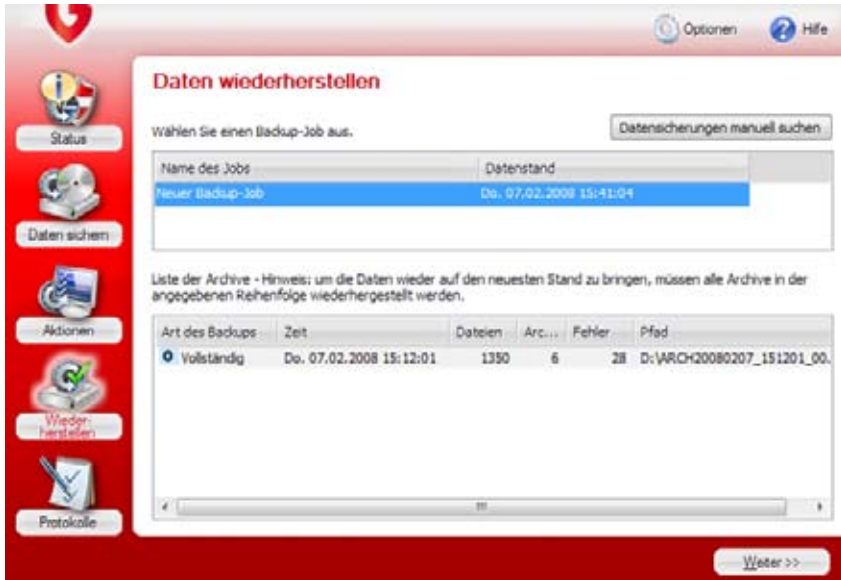


Folgende Aktionen und Dienstprogramme stehen Ihnen hierzu zur Verfügung:

- **Daten sichern:** Dieser Button führt Sie in den Bereich „**Daten sichern**“. Hier können Sie dann den gewünschten Backup-Job auswählen und über den Button „**Datensicherung starten**“ direkt aktivieren.
- **Daten wiederherstellen:** Dieser Button führt Sie in den Bereich „**Wiederherstellen**“. Hier können Sie dann die archivierten Daten des jeweiligen Backup-Jobs auswählen und über den Button „**Weiter**“ mit der Wiederherstellung beginnen.
- **Daten von Online-Backups pflegen:** Wenn Sie Ihre wichtigsten Daten auf einem FTP-Server sichern, braucht Backup natürlich die entsprechenden Zugangsdaten. Hier können Sie Host-Adresse, Port, Login, Passwort und alle anderen notwendigen Daten eingeben, die Ihnen mit der Registration zur Verfügung gestellt wurden oder die Sie von Ihrem FTP-Zugangsanbieter bekommen haben.
- **Daten nachträglich brennen:** Sie können Backup-Dateien auch nachträglich auf CD oder DVD brennen. Suchen Sie dazu einfach im erscheinenden Dialogfenster ein Projekt aus, welches Sie brennen möchten und klicken dann auf den **Brennen**-Button.
- **Ältere Datensicherungen löschen:** Wenn Sie ältere Datensicherungen nicht automatisch löschen lassen, können Sie diese hier manuell löschen. Suchen Sie dazu im erscheinenden Dialogfenster die nicht mehr benötigten Backup-Dateien auf Ihrem Wechselmedium oder dem FTP-Server heraus und klicken dann auf den **Löschen**-Button. Die letzte Datensicherung vor dem letzten vollständigen Backup kann nicht gelöscht werden.

■ Wiederherstellen

Im Wiederherstellen-Bereich können Sie auf Basis der gesicherten Backup-Daten Ihre Originaldateien nach einem Datenverlust wiederherstellen. Wählen Sie dazu den gewünschten Backup-Job unter **„Name des Jobs“** aus und wählen dann unter **„Art des Backups“** das gewünschte Archiv aus. Wenn Sie nun auf **„Weiter“** klicken, unterstützt Sie **Backup** bei der Wiederherstellung Ihrer archivierten Daten.



- Sie können die Datensicherungen über den Button „Datensicherungen manuell suchen“ auch unabhängig vom damit assoziierten Backup-Job suchen. Üblicherweise befinden sich die Archivdateien im Zielordner der letzten Datensicherung.

Wenn Sie eine Datensicherung ausgewählt und **„Weiter“** geklickt haben, werden Sie nun gefragt, ob Sie alle Dateien (**„Alles wiederherstellen“**) oder nur ausgewählte Dateien (**„Nur einzelne Dateien wiederherstellen“**) wiederherstellen möchten. Treffen Sie hier Ihre Auswahl, nennen Sie ggf. einen neuen Speicherort für die wiederhergestellten Dateien und klicken dann auf **„Wiederherstellung starten“**. Ihre Daten werden nun am angegebenen Ort wiederhergestellt.

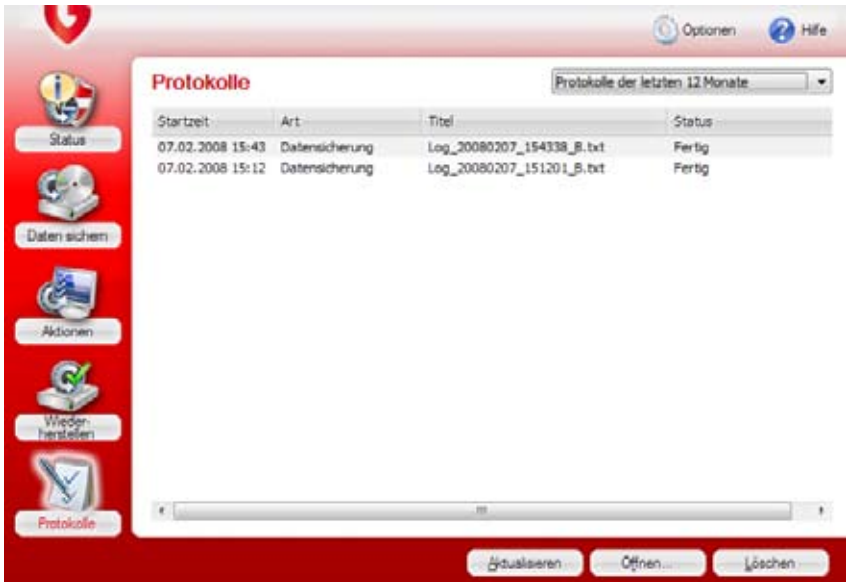
Daten wiederherstellen

☒ Alles wiederherstellen ☐ Nur einzelne Dateien wiederherstellen

- Wenn Sie statt des Buttons „Wiederherstellung starten“ den Button „nur Testen“ anklicken, erhalten Sie eine Info darüber, welches Ergebnis eine mögliche Wiederherstellung hätte.

■ Protokolle

Der Protokolle-Bereich stellt für jede Aktion und jeden Backup-Job eine umfangreiche **Log-Datei** bereit.



Hier können Sie einzelne Aktionen mit Doppelklick öffnen und gegebenenfalls ausdrucken oder als Textdatei abspeichern.

■ Einführung

Das Programm **TopSecret** ist sowohl für private Anwender im häuslichen Bereich als auch für kleine, mittelständische und große Unternehmen vorgesehen. Er dient der Absicherung von sensiblen Daten mit Hilfe sehr starker Verschlüsselungsalgorithmen. Zu den Programmfeatures gehört auch das Übertragen der Datensafes auf tragbare Wechselmedien wie z.B. CD/DVD oder Flash-Speichermedien wie z.B. USB-Sticks. Der Zugang zu den im Safe abgelegten Daten ist auf drei verschiedene Arten (z.B. mit Passwort) gegeben. Der Zugang zu der Verwaltungsebene des Programms kann auf drei verschiedene Arten abgesichert werden: mit einem Passwort, mit einem Sicherheitszertifikat oder mit einem Fingerabdruck. Das Programm verfügt über ein Passwortschutzmodul, welches das Ausspionieren von Passwörtern unmöglich macht.

■ Angewandte Technologie

Bei der Programmversion liegt das Hauptaugenmerk auf den Absicherungsmethoden vor Datendiebstahl oder dem Eindringen ins Computersystem von intern oder extern.

Methoden der Authentifizierung

Der Zugang zur Safeverwaltung als auch zum Safe selbst kann auf drei unterschiedliche Weisen abgesichert werden - mit Passwort, mit Sicherheitszertifikat oder mit Hilfe eines biometrischen Lesegerätes (Fingerabdruck). Zu der letztgenannten Methode der Authentifizierung ist ein spezielles biometrisches Lesegerät (z.B. von UPEK Inc.) erforderlich, das das Einloggen mit Fingerabdruck ermöglicht.

Absicherung vor der Passwortübernahme

Während des Einloggens ins Programm oder in den angelegten Datensafe sowie bei der Eingabe eines neuen Passwortes wird automatisch ein Schutzmechanismus aktiviert, welcher das „Abhören“ von Passwörtern verhindert. Im Login-Fenster erscheint dann der Hinweis **„Der Schutz vor Spionageprogrammen ist aktiv“**. Spionageanwendungen wie z.B. Keylogger können Passwörter übernehmen, die über Tastatur eingetippt werden. **TopSecret** schützt effektiv vor solchen Eingriffsversuchen.

Speichern auf Wechseldatenträgern

Mit Hilfe der Option **„Portablesafe erstellen“** kann der Safe auf beliebige Wechseldatenträger gespeichert werden.

Bei Wechselspeichermedien, die mit einer Seriennummer ausgestattet sind, z.B. Wechselsfestplatten oder USB-Sticks gibt es zusätzlich die Möglichkeit, den Safe mit dem jeweiligen Datenträger zu verknüpfen. Dies schützt den Safe vor dem Öffnen oder Kopieren auf einem anderen Datenträger. Der so verknüpfte Safe kann nur auf dem Medium geöffnet werden, auf dem er ursprünglich erstellt wurde.

Wenn der Safe also auf einer Festplatte eines Laptops oder Desktop-PCs erstellt wurde und mit dieser Festplatte verknüpft ist, kann man ihn nur auf diesem Laptop oder Desktop-PC öffnen.

Wenn man den Safe auf einem USB-Stick oder sonstigen tragbaren Festplatten (vorausgesetzt diese haben eine Seriennummer) erstellt und ihn mit diesem USB-Stick oder dieser tragbaren Festplatte verknüpft, wird es künftig möglich sein, den Safe ausschließlich auf diesem Wechselmedium in anderen Computern zu öffnen.

■ Verschlüsselungsalgorithmus

Das Programm **TopSecret** ermöglicht es, Datensafes unterschiedlicher Größe zu erstellen. Der Datensafe stellt einen mit einem Algorithmus verschlüsselten Bereich auf der Festplatte dar. Der Safeadministrator legt bei der Safeerstellung die Datengröße, Zugangsberechtigung sowie den Verschlüsselungsalgorithmus fest. Die bei dem Programm verwendeten Algorithmen gehören zu den sichersten Verschlüsselungsalgorithmen und wurden vom NIST (National Institute of Standards and Technology) als fortgeschrittene Verschlüsselungsstandards (AES=Advanced Encryption Standard) weltweit anerkannt.

- **MARS:** Auch IBM nahm mit seiner Chiffre MARS an der Ausschreibung zum AES teil. Der Algorithmus schaffte es bis in die finale Runde des Auswahlverfahren und gilt nach heutigen Erkenntnisstand als sicher. Die Grundstruktur des Algorithmus bildet ein Feistelnetzwerk. Diese spezielle Struktur garantiert auch die Umkehrbarkeit des Algorithmus zwischen der Ver- und Entschlüsselung. MARS bietet variable Schlüssellängen von 128 bis 448 Bit, wobei die Schlüssellänge ein Vielfaches von 32 Bit sein muss.
- **RC6:** RC6 (Rivest Cipher Version 6) ist ein Blockverschlüsselungsverfahren (Blockchiffre), das 1998 als einer der 15 Kandidaten für den Advanced Encryption Standard veröffentlicht wurde. Es wurde von Ron Rivest, Matt Robshaw, Ray Sidney und Yiqun Li Yin entwickelt. Es unterstützt variable Schlüssellängen von 128, 192 und 256 Bit und arbeitet mit einer Blocklänge von 128 Bit. Der Algorithmus ist sehr schnell und einfach zu implementieren. In den Geschwindigkeitstests belegte er den ersten Platz.
- **Rijndael:** Nach seinen Entwicklern Joan Daemen und Vincent Rijmen wird er auch Rijndael-Algorithmus genannt (gesprochen wie dt. „Rheindahl“). Der Rijndael-Algorithmus besitzt eine variable Blockgröße von 128, 192 oder 256 Bit und eine variable Schlüssellänge von 128, 192 oder 256 Bit. Rijndael bietet ein

sehr hohes Maß an Sicherheit. Das Verfahren wurde eingehenden kryptoanalytischen Prüfungen unterzogen. AES schränkt die Blocklänge auf 128 Bit ein, während die Wahl der Schlüssellänge von 128, 192 oder 256 Bits unverändert übernommen worden ist. Anhand der Schlüssellänge wird zwischen den drei AES-Varianten AES-128, AES-192 und AES-256 unterschieden.

- **Serpent:** Serpent ist ein symmetrischer Verschlüsselungsalgorithmus, der von den Kryptografen Ross Anderson, Eli Biham und Lars Knudsen entwickelt wurde. Dieser Algorithmus war ein Kandidat für den Advanced Encryption Standard und gehörte mit Twofish und Rijndael zu den drei Finalisten. Serpent ist eine Blockchiffre mit einer Blockgröße von 128 Bit und kann mit jeder Schlüsselgröße bis 256 Bit umgehen. Der Algorithmus arbeitet anders als Twofish über 32 Runden (Twofish: 16 Runden) und operiert auf Blöcken von vier 32-Bit-Worten. Durch die Verwendung von 32 Runden ist Serpent etwas langsamer als andere Algorithmen.
- **Twofish:** Twofish ist ein symmetrischer Verschlüsselungsalgorithmus, der von Bruce Schneier, Niels Ferguson, John Kelsey, Doug Whiting, David Wagner und Chris Hall mitentwickelt wurde. Er stellt den Nachfolger von Blowfish dar und stellte sich 1998/1999 dem Ausscheid zum Advanced Encryption Standard. Dort kam er zusammen mit Rijndael und Serpent in die Runde der letzten drei. Twofish ist eine Blockchiffre mit einer Blockgröße von 128 Bit und 16 Runden. Es arbeitet mit Schlüssellängen von 128-, 192- und 256 Bit.

■ Erster Programmstart

Beim ersten Programmstart von **TopSecret** muss das Administratorkonto erstellt werden. Das Programm öffnet dazu automatisch ein Auswahlfenster mit möglichen Zugangsmethoden für den Administrator. Die Zugangsmethode für den Administrator kann geändert werden, indem die entsprechend beschriebene Taste der Zugangsmethode gedrückt wird. Der Programmadministrator verfügt über alle Zugangsmöglichkeiten (Authentisierung) gleichzeitig.

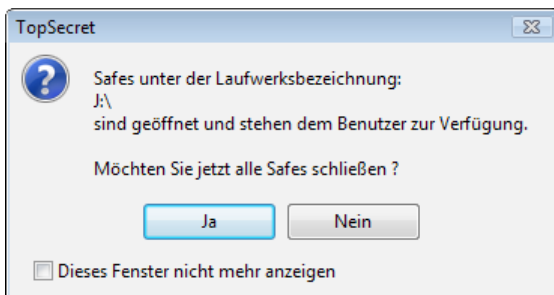
Die Authentifizierung (engl. authentication) bezeichnet den Vorgang der Überprüfung der Identität eines Gegenübers (in diesem Falle einer Person). Die Authentisierung dagegen bezeichnet den Vorgang des Nachweises der eigenen Identität.

Bei einer Identitätsüberprüfung oder Identifizierung gibt es daher immer einen Teilnehmer, der sich authentisiert und einen, der diesen authentifiziert. In einem Computerprogramm werden einer Identität (das heißt einer identifizierten Person) üblicherweise Rechte zugeordnet. Autorisierung bezeichnet den Vorgang, mit dem ein Computerprogramm prüft, ob eine bestimmte Identität ein bestimmtes Recht besitzt (und damit zum Beispiel eine bestimmte Aktion ausführen darf).

Die Authentisierung, das heißt das Nachweisen der eigenen Identität, kann bei **TopSecret** auf drei verschiedenen Wegen erfolgen. Die jeweiligen Zugangsmethoden werden in folgenden Kapiteln detailliert beschrieben:

- Einloggen mit Passwort
- Einloggen mit Sicherheitszertifikat
- Einloggen mit biometrischem Lesegerät

■ Bei dem Versuch, **TopSecret** zu schließen, während noch ein Safe geöffnet ist, erscheint eine Frage, ob die Anwendung alle geöffneten Safes schließen soll.



Wenn Sie nicht möchten, dass dieser Hinweis künftig erscheint, markieren Sie bitte das Feld „**Dieses Fenster nicht mehr anzeigen**“.

■ Einloggen mit Passwort

Die einfachste Zugangsmethode bietet das Passwort. Das Passwort sollte aus großen und kleinen Buchstaben sowie mindestens einer Zahl bestehen. Die minimale Passwortlänge beträgt acht Zeichen. Wenn Sie das Passwort vergessen, können Sie sich nicht mehr in das Programm einloggen.

Im Moment der Passwortvergabe als auch während des Einloggens mit dem Passwort sollte im Fenster die folgende Information eingeblendet werden: „**Der Schutz vor Spionageprogrammen ist aktiv**“. Wenn das nicht der Fall ist, dann ist die Passworтеingabe nicht sicher. In diesem Fall empfehlen wir einen Computerneustart.



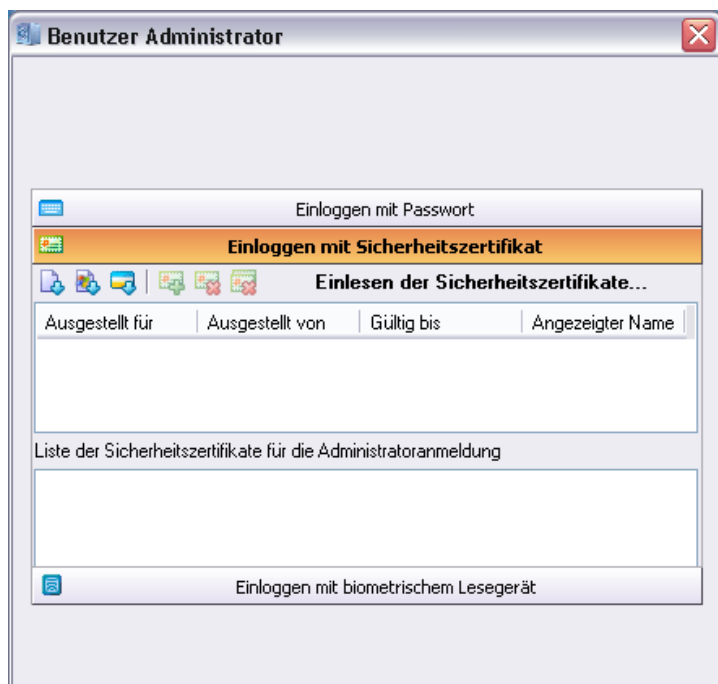
■ Einloggen mit Sicherheitszertifikat

Um sich mit einem Sicherheitszertifikat einloggen zu können, muss der Benutzer ein digitales Zertifikat und einen dazugehörigen privaten Schlüssel besitzen. So ein Zertifikat befindet sich z.B. auf einer kryptografischen Smartcard. Das Sicherheitszertifikat kann von einer abgelegten Datei, einer Sammelstelle für Windowszertifikate oder eben einer solchen kryptografischen Smartcard eingelesen werden. Die kleinen Symbole in der Werkzeugleiste des Login-Fensters mit Hilfe der Sicherheitszertifikaten ermöglichen (von links nach rechts):



- Einlesen des Zertifikats von einer Datei
- Einlesen des Zertifikats von einer Sammelstelle der Windows Zertifikate
- Einlesen des Zertifikats von einer kryptografischen Smartcard

- Hinzufügen des eingelesenen Zertifikates zu Liste von **TopSecret**
- Löschen des eingelesenen Zertifikates aus der Liste
- Löschen aller Zertifikate aus der Liste



■ Einloggen mit biometrischem Lesegerät

Um sich als Benutzer des Programms mit Hilfe des Fingerabdrucks authentifizieren zu können, ist ein zusätzliches Fingerabdrucklesegerät erforderlich. **TopSecret** unterstützt dabei eine große Anzahl biometrischer Lesegeräte (z.B. von UPEK Inc.). Beim ersten Start dieser Zugangsmethode fordert die Anwendung zweimalig einen Fingerabdruck.

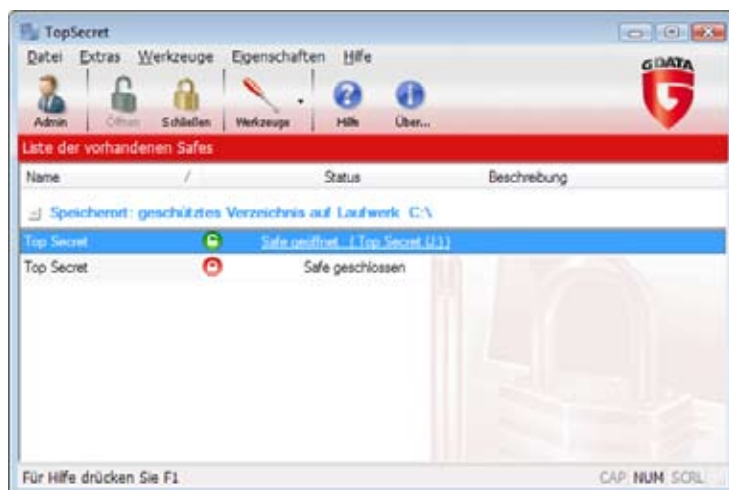
Nach erfolgreicher Probenahme und dem Vergleich der beiden Proben miteinander, wird der Benutzer gebeten, die **neue Zugangsmethode** zu **speichern**.



■ Administratorkonto

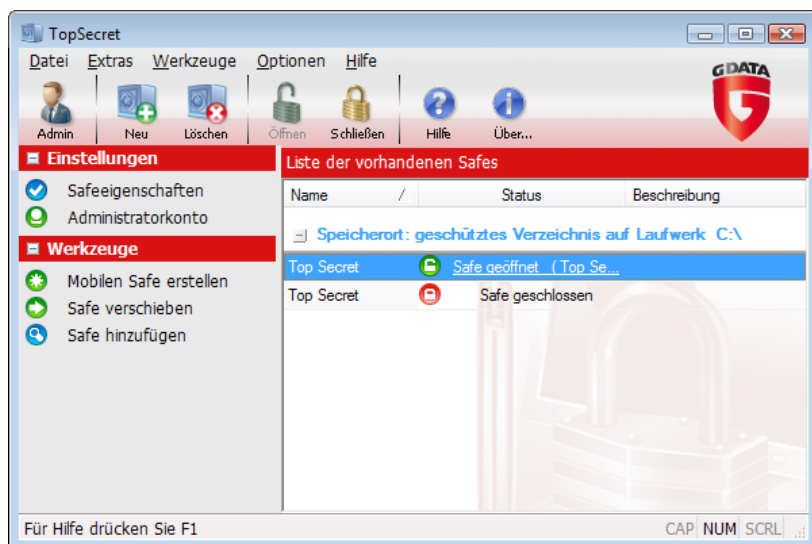


Um Einstellungen als Administrator vorzunehmen, klicken Sie einfach auf das Symbol „**TopSecret starten**“ auf Ihrem Desktop. Nun öffnet sich die Programmoberfläche.





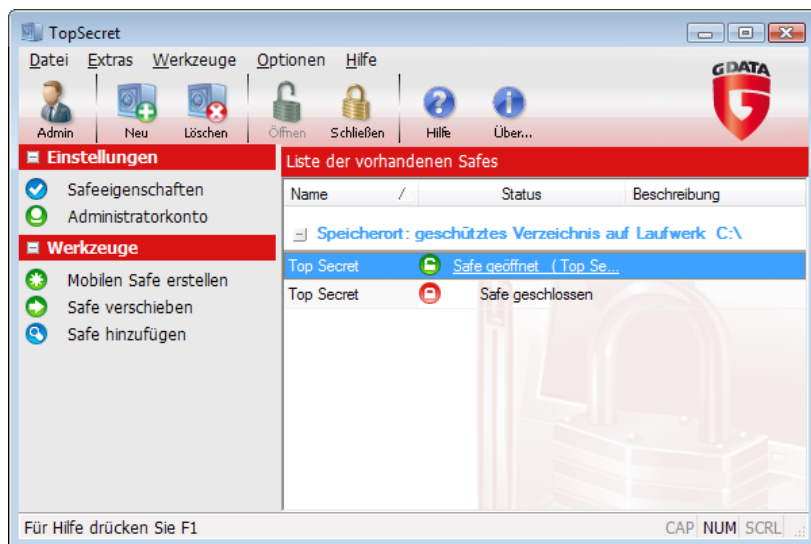
Im Gegensatz zu Anwendern, die keine Administratorrechte besitzen, können Sie mit Anklicken des Buttons „**Admin**“ weitergehende Einstellungen von TopSecret verändern und die Tresore der einzelnen Benutzer verwalten.



■ Programmaufbau

Nach dem Einloggen ins Programm in der Menüleiste stehen Ihnen folgende Funktionen zur Auswahl: Ohne Administratorrechte kann der User den Safe lediglich öffnen und schließen sowie einen **mobilen Safe** erstellen. Darunter befindet sich die Werkzeugleiste des Programms **TopSecret**. Unter der Werkzeugleiste befindet sich eine Liste, in welcher die bereits vorhandenen Safes angezeigt werden. Werkzeuge der Safeverwaltung erscheinen links nach dem Einloggen als Administrator.

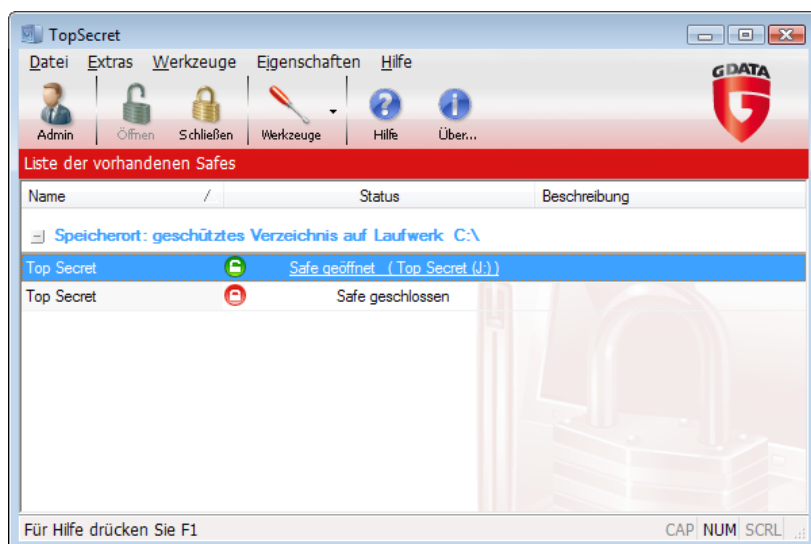
Ganz unten im Kontextmenü der Statusleiste erscheint ein Hinweis auf die Hilfe über das markierte Element. Rechts davon erscheinen Tastaturhinweise, die über eingeschaltete Tasten informieren.



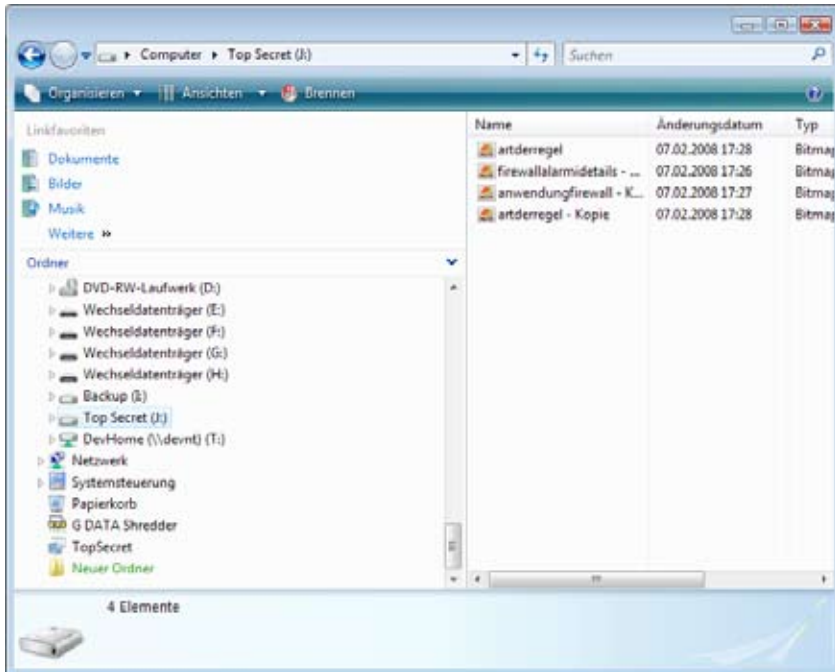
■ Desktopverknüpfung



Um Einstellungen als Administrator vorzunehmen, klicken Sie einfach auf das Symbol „**TopSecret starten**“ auf Ihrem Desktop. Nun öffnet sich die Programmoberfläche. Hier können Sie geschlossene Safes öffnen, verwalten und ggf. löschen.



Ein geöffneter Safe wird im Windows Explorer oder anderen Dateimanagern wie eine eigene Festplatten-Partition oder ein Laufwerk mit einem Laufwerksbuchstaben angezeigt. Dateioperationen wie z.B. Kopieren, Verschieben, Löschen und Erstellen können dabei ganz normal durchgeführt werden, solange der Safe geöffnet ist.



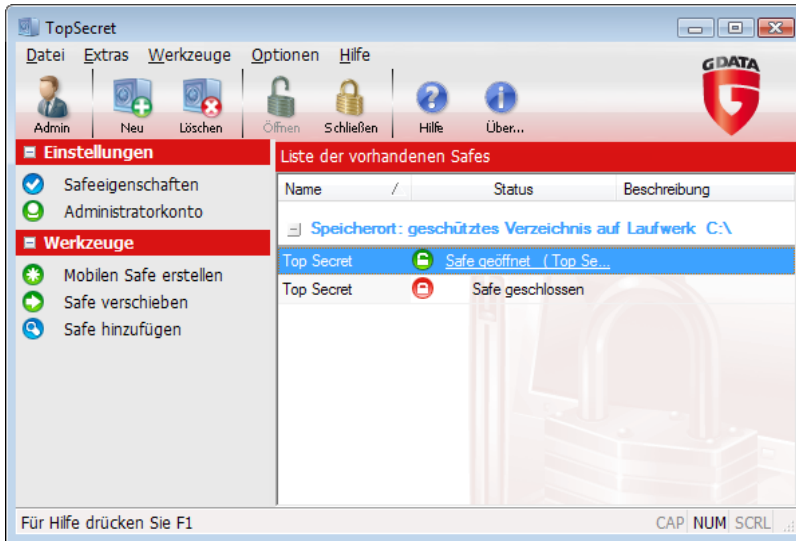
Hauptfenster



Die Benutzeroberfläche des Programms wird über das Menü „**Start** > **Alle Programme** > **G DATA Software** > **TopSecret**“ gestartet oder über das Desktopsymbol „**TopSecret starten**“.



Um sich als Programmadministrator einzuloggen, drücken Sie bitte die Taste „**Admin**“ in der Werkzeugleiste des Programms.



Die linke Spalte ermöglicht die Safeverwaltung - also die Durchführung aller angebotenen Programmoperationen an den Safes:

- **Safeeigenschaften:** Dieser Button öffnet das Programmfenster mit Safeeigenschaften und -berechtigungen (Allgemein und Zugang).
- **Administratorkonto:** Dieser Button öffnet ein Dialogfenster, über welches der Administrator Passwörter für jeweilige Safes ändern kann. Das geöffnete Dialogfenster ermöglicht ebenfalls eine Änderung der Zugangsmethoden zum Administratorkonto.
- **Mobilen Safe erstellen:** Diese Option ist aktiv, wenn der bereits erstellte Safe markiert wird. Sie bietet die Möglichkeit, einen portablen Safe zu erstellen, welcher auf CD, DVD oder USB-Stick aufgenommen werden kann.
- **Safe verschieben:** Mit Hilfe dieses Befehls kann der bereits existierende Datensafe in ein ausgewähltes Verzeichnis, auf eine andere vom Benutzer ausgesuchte Festplatte oder andere Festplattenpartition des geschützten Verzeichnisses verschoben werden.
- **Safe hinzufügen:** Dieser Befehl ermöglicht, bereits vorhandene Safes, die mit Hilfe des Programms **TopSecret** noch vor der letzten Programminstallation erstellt wurden, in das aktuelle Programm hinzuzufügen. Diese Befehl ist sehr hilfreich, wenn das Programm z.B. wegen Systemfehlern, Hardwarefehlern, etc. neu installiert werden musste. Auf diese Weise, werden die auf der Festplatte vorhandenen Safes manuell hinzugefügt.

■ Menüleiste

Sämtliche Befehle aus der Menüleiste sind erst nach dem Einloggen als Administrator verfügbar.

Datei Extras Werkzeuge Optionen Hilfe

Datei

- **Beenden:** Schließt das Programmfenster von **TopSecret**.

Extras

- **Administrator anmelden:** Öffnet das Login-Fenster des Programmadministrators. Der Administrator des Programms kann sich mit Passwort, Sicherheitszertifikat oder mit biometrischem Lesegerät anmelden.
- **Administrator abmelden:** Meldet den Programmadministrator ab.
- **Safe neu:** Dieser Befehl startet den Safeaufbauassistenten
- **Safe löschen:** Dieser Befehl ermöglicht, den Safe ohne die vorherige Passworteingabe zu löschen.
- **Safe öffnen/schließen:** Öffnet oder schließt den erstellten Safe. Um den Safe zu öffnen, ist die Passworteingabe des Safebenutzers erforderlich.
- **Autosafes öffnen:** Die Funktion „Autosafes“ ermöglicht es, alle zuvor auf dem PC angelegten Safes auf einen Schlag zu öffnen. Dies ist dann möglich, wenn die zuvor angelegten Safes, die Eigenschaft „Autosafe“ zugewiesen bekommen haben. Wenn man also mehrere Safes auf dem Rechner hat, werden sie alle mit dieser Funktion automatisch eröffnet. Dies setzt voraus, dass die zuvor angelegten Safes, die gleiche Zugangsmethode (also z.B. Passwort oder Sicherheitszertifikat) haben. Wie Sie einen Autosafe erstellen, lesen Sie im Kapitel „Safezugang - Berechtigung“.

Werkzeuge

- **Mobilen Safe erstellen:** Diese Option ist nach dem Markieren des ausgesuchten Safes aktiv. Sie ermöglicht, einen mobilen Safe zu erstellen, welcher auf CD / DVD oder USB-Stick aufgenommen wird.
- **Safe verschieben:** Mit Hilfe dieses Befehls kann der bereits existierende Datensafe in ein ausgewähltes Verzeichnis, auf eine andere vom Benutzer ausgesuchte Festplatte oder andere Festplattenpartition des geschützten Verzeichnisses verschoben werden.
- **Einstellungen:** Dieser Befehl ermöglicht, bereits vorhandene Safes, die mit Hilfe des Programms **TopSecret** noch vor der letzten Programminstallation erstellt wurden, in das aktuelle Programm hinzuzufügen. Dieser Befehl ist sehr hilfreich,

wenn das Programm z.B. wegen Systemfehlern, Hardwarefehlern, etc. neu installiert werden musste. Auf diese Weise, werden die auf der Festplatte vorhandenen Safes manuell hinzugefügt.

Optionen

- **Eigenschaften:** Dieser Button öffnet das Fenster mit Safeeigenschaften und -berechtigungen.
- **Benutzerkonto: Administrator:** Dieser Button öffnet ein Dialogfenster, über welches der Administrator Passwörter für jeweilige Safes ändern kann. Das geöffnete Dialogfenster ermöglicht ebenfalls eine Änderung der Zugangsmethoden zum Administratorkonto.

Hilfe

- **TopSecret - Hilfe:** Öffnet die Programmhilfe zu **TopSecret**.
- **TopSecret - Information:** Zeigt Informationen über die Programmversion an.

■ Werkzeugleiste

Die Werkzeugleiste bietet einen schnellen Zugang zu einigen Hauptbefehlen von **TopSecret**.



- **Admin anmelden/abmelden:** Safeadministrator an- und abmelden.
- **Neu:** Ermöglicht es einen neuen Safe zu erstellen.
- **Löschen:** Löscht den markierten Safe.
- **Öffnen/Schließen:** Öffnet oder schließt den Safe
- **Hilfe:** Öffnet die Hilfedatei des Programms **TopSecret**.
- **Über:** Zeigt Informationen über die Programmversion an.

■ Safefenster

Im Safefenster werden alle Safes angezeigt, die mit dem Programm **TopSecret** erstellt wurden.

Name	Status	Beschreibung
- Speicherort: geschütztes Verzeichnis auf Laufwerk C:\		
Top Secret		Safe geschlossen
Top Secret		Safe geöffnet (Top Secret (J:))

Das Fenster zeigt die Safelokalisierung, Safenamen sowie die Safebeschreibung an und gibt Auskunft darüber, ob der Safe geöffnet oder geschlossen ist.

■ Safes

TopSecret ermöglicht die sichere Aufbewahrung von Daten in virtuellen Safes. Der Programmsadministrator kann eine beliebige Anzahl von Safes für unterschiedliche Computerbenutzer erstellen. Die Computerbenutzer können unterschiedliche Zugangsdaten sowie unterschiedliche Benutzerrechte zugewiesen bekommen. Die Einstellungsmöglichkeiten als Administrator sind einzeln in folgenden Kapiteln beschrieben:

- Safe erstellen
- Öffnen und Schließen von Safes
- Mobiler Safe
- Safe verschieben
- Safeinformation hinzufügen
- Safeeigenschaften

■ Safe erstellen

Nach dem Einloggen ins Programm kann der Benutzer mit der Safeerstellung beginnen. Der Safeaufbauassistent führt Sie durch die Erstellungsprozedur. Der Safeaufbauassistent startet beim Drücken des Buttons „**Neu**“ in der Werkzeugleiste.



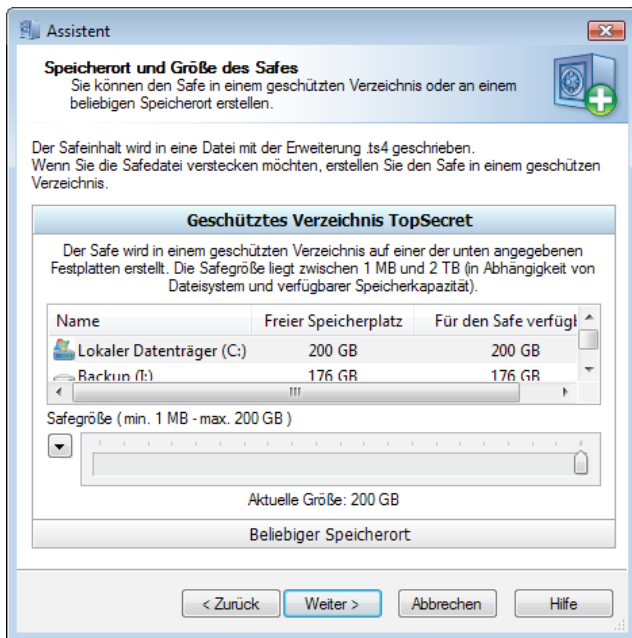
Safeerstellung im geschützten Verzeichnis

Safe im geschützten TopSecret-Verzeichnis anlegen

Das Programm bietet standardmäßig die Option an, den Safe in einem geschützten Verzeichnis einer ausgewählten Festplattenpartition zu erstellen. Sollte das Programm nicht standardmäßig auf dieser Option eingestellt sein, klicken Sie einfach auf den Button „Geschütztes Verzeichnis TopSecret“.

■ **Achtung: Dieses Verzeichnis wird unter Windowssystemen ohne TopSecret nicht sichtbar sein!**

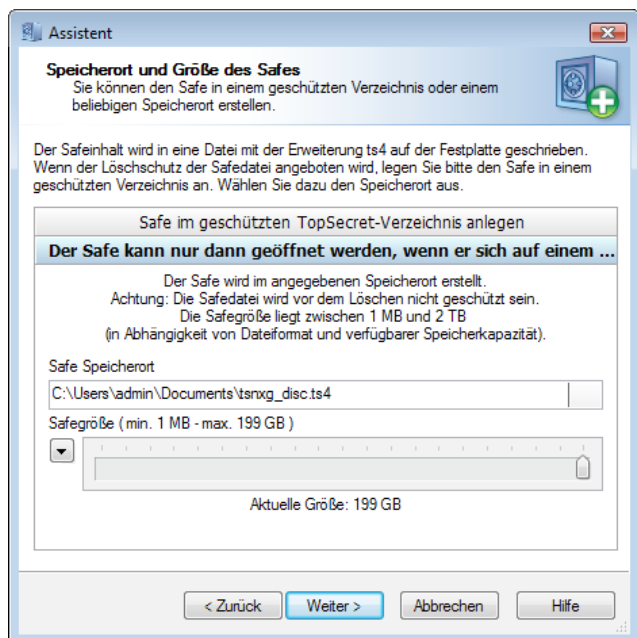
Wählen Sie eine Festplattenpartition aus, auf welcher das Safeverzeichnis erstellt werden soll. Das Programm informiert über die vorhandenen Partitionen sowie den verfügbaren Speicherplatz. Darunter befindet sich ein Schieber, mit Hilfe dessen die Safegröße eingestellt werden kann. Wenn man den Pfeil links davon drückt, erscheint ein Eingabefeld, mit Hilfe dessen die genaue Safegröße eingegeben werden kann. Der Benutzer kann hier die genaue Angabe über die Safegröße in MB vornehmen oder eine vom Programm vorgegebenen Größen übernehmen. Drücken Sie „**WEITER**“ um fortzufahren.



Achtung: Beim Erstellen eines neuen Safes reservieren Sie auf der Festplattenpartition den entsprechenden Platz ausschließlich für diesen Safe. Natürlich steht Ihnen dieser Platz auf der Partition wieder zur Verfügung, wenn Sie den Safe wieder löschen oder entfernen, aber mit dem Erstellen des Safes ist der Platz auf der Festplatte erst einmal reserviert. Gerade dann, wenn Sie den Safe auf Ihrer Windows-Partition erstellen oder z.B. einen Rechner haben, auf dem nur eine Partition/Festplatte vorhanden ist (in der Regel das Laufwerk „C:“), sollten Sie den Safe nicht in der Maximalgröße anlegen. Generell ist es sinnvoll, auf der Festplatte, auf der Ihr Windows-Betriebssystem läuft, etwa 2 GB freien Speicherplatz zu reservieren, also sollten Sie Ihren Safe z.B. bei einer möglichen Maximalgröße von 300 GB maximal auf 298 GB Größe einstellen. In der Regel benötigen Ihre persönlichen Daten deutlich weniger Platz.

Safeerstellung an beliebigem Speicherort

Der Benutzer des Programms kann aber auch den zu erstellenden Safe an einem Ort seiner Wahl anlegen. Klicken Sie zur Auswahl dieser Option auf den Button „**Beliebiger Speicherort**“. Analog zur Safeerstellung im geschütztes Verzeichnis muss auch hier die Safegröße festgelegt werden. Drücken Sie „**WEITER**“ um fortzufahren.



■ Safezugang - Einstellung

Im nachfolgenden Fenster können der Safename sowie die Beschreibung eingetragen werden. Hier sollte der Benutzer den Verschlüsselungsalgorithmus seiner Wahl und das Dateiformat (FAT oder NTFS) festlegen. Das Programm kann automatisch einen Laufwerksbuchstaben wählen. Der Benutzer kann aber den Laufwerksbuchstaben auch selber (manuell) aussuchen.

Nachdem die erforderlichen Einstellungen vorgenommen worden sind, erscheint ein Fenster mit Zugangseinstellungen des Safes.

Der Safezugang ist auf dreifache Weise geschützt: mit Passwort, mit Sicherheitszertifikat oder mittels biometrischem Lesegerät.

Für die letztgenannte Zugangsmethode ist ein spezielles Lesegerät erforderlich (z.B. von UPEK Inc.).

Im Moment der Eingabe eines neuen Passwortes als auch während des späteren Einloggens mit Passwort sollte im Fenster die Information eingeblendet werden: **„Der Schutz vor Spionageprogrammen ist aktiv“**. Wenn das nicht der Fall ist, dann ist die Passwordeingabe nicht sicher. In diesem Fall empfehlen wir einen Computerneustart.

Assistent

Safeparameter
Der Safename, die Art des Zugangs sowie der Verschlüsselungsalgorithmus

Geben Sie den Safenamen für Windows Explorer an, wählen Sie den Verschlüsselungsalgorithmus und andere Safeparameter.

Allgemein	
Safebezeichnung	Top Secret
Beschreibung	
Verschlüsselungsalgorithmus	AES (Rijndael)
Dateisystem	Automatische Auswahl
Safelaufwerk	
Safelaufwerk automatisch wählen	Ja
Laufwerk zuordnen	Nur freie Laufwerke
Auswahl: K:\	

Safebezeichnung
Legt die Bezeichnung fest, unter welcher der Safe im System angezeigt wird

< Zurück Weiter > Abbrechen Hilfe

Assistent

Safezugang
Legen Sie die Zugangsart und die Zugangsberechtigung zum Safe fest.

Der Zugang zum Safe erfolgt durch die Eingabe von: Passwort, Sicherheitszertifikat oder Fingerabdruck. Der Safe kann mit mehreren Passwörtern betrieben werden, von denen jedes Passwort eine andere Berechtigung besitzen kann.

Safezugang mit Passwort

 [Der Schutz vor Spionageprogrammen ist aktiv](#)

Passwortangabe. Um ein Passwort hinzuzufügen, drücken Sie "Hinzufügen". Mehrfachangaben sind möglich.

Hinzufügen Löschen Berechtigung

Name		Administratorechte

Safezugang mit Sicherheitszertifikat

Safezugang mit biometrischem Lesegerät

< Zurück Weiter > Abbrechen Hilfe

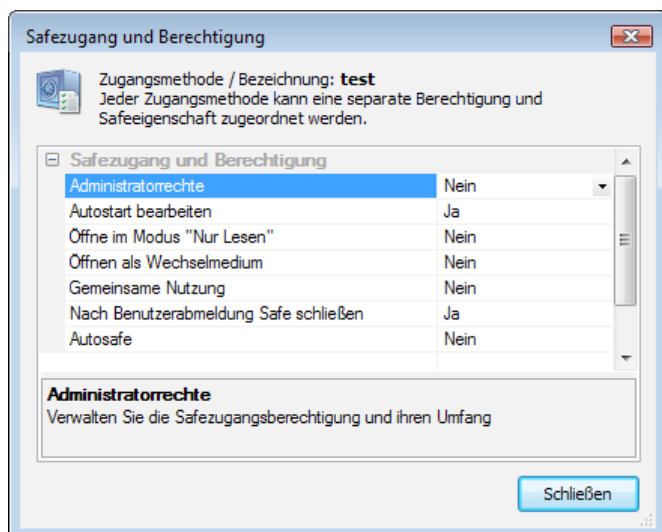
Wenn sich der Programmbenutzer für den Safezugang per Sicherheitszertifikat oder biometrischem Lesegerät entschieden hat, ist die Vorgehensweise analog zu:

- Einloggen mit Sicherheitszertifikat
- Einloggen mit biometrischem Lesegerät

Die Zugangsmethode mit Passwort ist sehr ähnlich zum Einloggen als Administrator. Diese Methode ermöglicht zusätzlich die mehrfache Passwortvergabe. Für jeden Safe, welchen der Benutzer mit Hilfe dieses Programmes erstellt, können drei verschiedene Zugangsmethoden konfiguriert werden. Die Safezugang-Berechtigung ist das Thema des nächsten Kapitels

■ Safezugang - Berechtigung

Für jede Zugangsmethode und sogar für jedes Passwort kann eine unterschiedliche Safeberechtigung erteilt werden.



Das Fenster mit Berechtigungsoptionen erscheint nachdem das Eigenschaftenfenster für die jeweilige Zugangsart gewählt wurde.

- **Administratorrechte** : Das Markieren dieser Option ermöglicht dem Benutzer die spätere Änderungen der Safeeigenschaften. **ACHTUNG:** *Wenigstens eine der Safezugangsmethoden muss über Administratorrechte verfügen. Wenn das nicht*

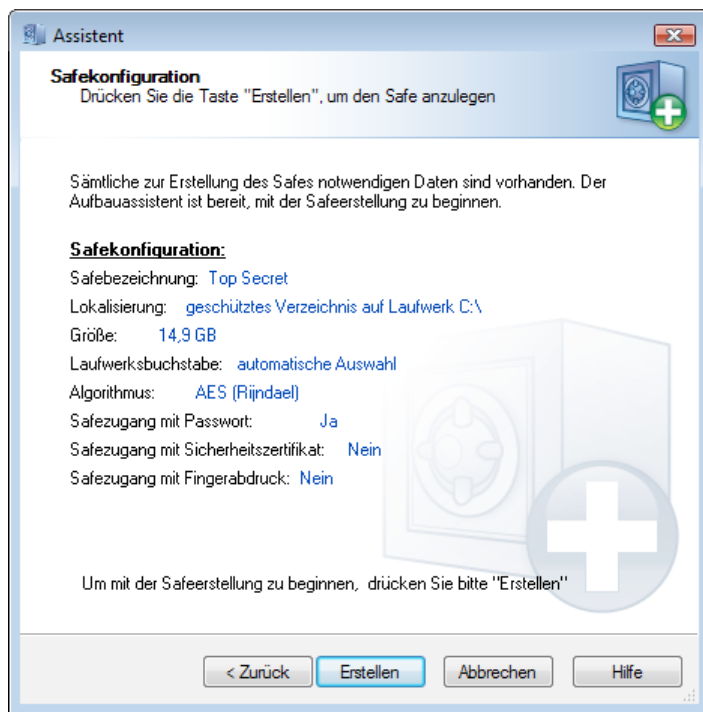
der Fall ist, wird eine Fehlermeldung in der Dialogbox des Programmes erscheinen. Der Übergang zum nächsten Programmschritt ist dann unmöglich. Das Fenster „**Safezugang und Berechtigung**“ wird dann automatisch geöffnet.

- **Autostart bearbeiten:** In jedem Safe befindet sich ein Verzeichnis mit dem Namen „**Autostart**“. Wenn diese Option auf „**JA**“ eingestellt bleibt, wird das Programm **TopSecret** beim Öffnen des Safes alle dort befindlichen ausführbaren Dateien starten.
- **Öffne im Modus „Nur lesen“:** Ein Benutzer, der sich mit dieser Zugangsmethode einloggt, wird die im Safe befindlichen Dateien weder speichern noch verändern können. Er kann sie lediglich lesen.
- **Öffnen als Wechselmedium:** **TopSecret** öffnet Datensafes im Explorer als lokale Festplatten. Wenn Sie möchten, dass der Safe als Wechseldatenträger im System sichtbar wird, markieren Sie bitte diese Option.
- **Gemeinsame Nutzung:** Das Markieren dieser Option ermöglicht die gemeinsame Nutzung des Safeverzeichnisses für andere Computer im Netzwerk.
WARNUNG: *Der Safezugang ist dann ohne die Notwendigkeit der Passworteingabe oder anderer Zugangsart möglich. Wir empfehlen an dieser Stelle eine vorsichtige und bewusste Wahl der gemeinsamen Nutzung des Safes. Die gemeinsame Nutzung des Safes für alle Netzwerkteilnehmer ist an dieser Stelle sinnlos, da in diesem Fall die Daten jedem zugänglich sind.*
- **Nach Benutzerabmeldung Safe schließen:** Diese Option sollte in der Regel aktiviert sein, denn wenn der Safe auch nach der Benutzerabmeldung offen bleibt, können andere Benutzer den Inhalt des Safes einsehen.
- **Autosafe:** Die Funktion „Autosafes“ ermöglicht es, alle zuvor auf dem PC angelegten Safes auf einen Schlag zu öffnen. Dies ist dann möglich, wenn die zuvor angelegten Safes, die Eigenschaft „**Autosafe**“ zugewiesen bekommen haben. Wenn man also mehrere Safes auf dem Rechner hat, werden sie alle mit dieser Funktion automatisch eröffnet. Dies setzt voraus, dass die zuvor angelegten Safes, die gleiche Zugangsmethode (also z.B. Passwort oder Sicherheitszertifikat) haben.

Nachdem Sie die erforderlichen Einstellungen vorgenommen haben, schließen Sie das Fenster und klicken auf Weiter.

■ **Safekonfiguration**

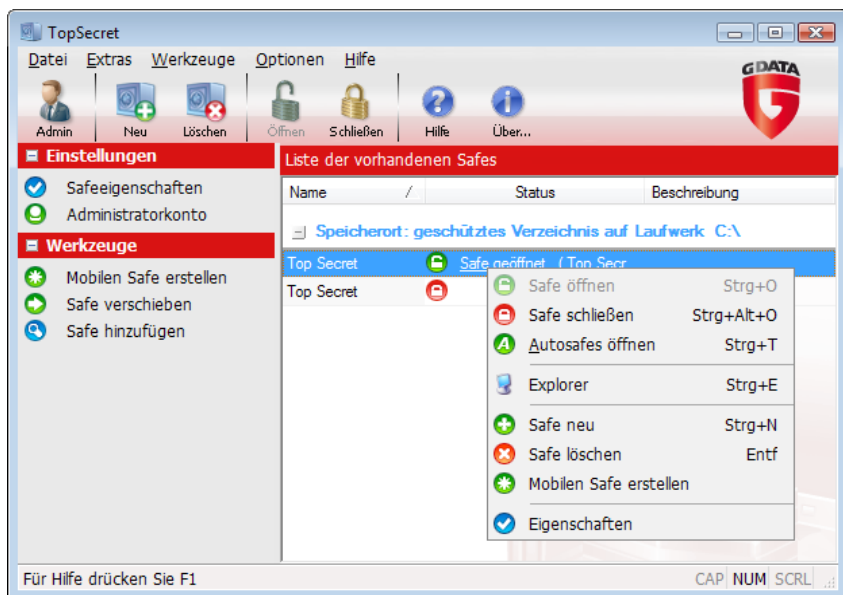
Der Safeaufbauassistent informiert Sie im letzten Schritt über die Einstellungsparameter.



Wenn Sie diese Einstellungen ändern möchten, klicken Sie bitte die Taste „**Zurück**“. Wenn Sie mit den Einstellungen zufrieden sind, klicken Sie bitte „**Erstellen**“. Der virtuelle und verschlüsselte Datensafe wird auf der Festplatte Ihres Computers erstellt.

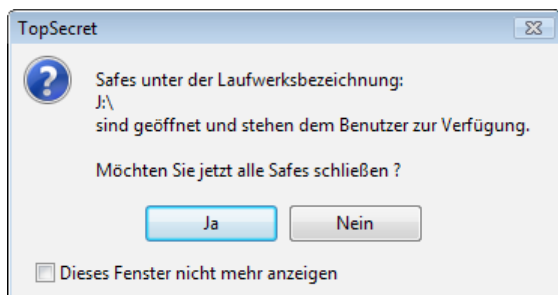
■ Öffnen und Schließen von Safes

Das Öffnen und Schließen des Safes ist sowohl vom Programmexplorer in Windows als auch vom Hauptfenster des Programms aus möglich. Sie können dazu die Werkzeugleiste oder das Kontextmenü der rechten Maustaste benutzen.



Das Schließen des Safes ist analog zum Öffnen auf zwei Arten möglich. Benutzen Sie im Kontextmenü den Befehl „**Safe schließen**“.

Beim Öffnen und Schließen des Safes als auch beim Beenden des Programms **TopSecret** bei geöffneten Safes erscheint ein Hinweis, der über das Öffnen oder Schließen der Safes informiert.



Wenn Sie nicht möchten, dass dieser Hinweis künftig erscheint, markieren Sie das Feld „**Dieses Feld nicht mehr anzeigen**“.

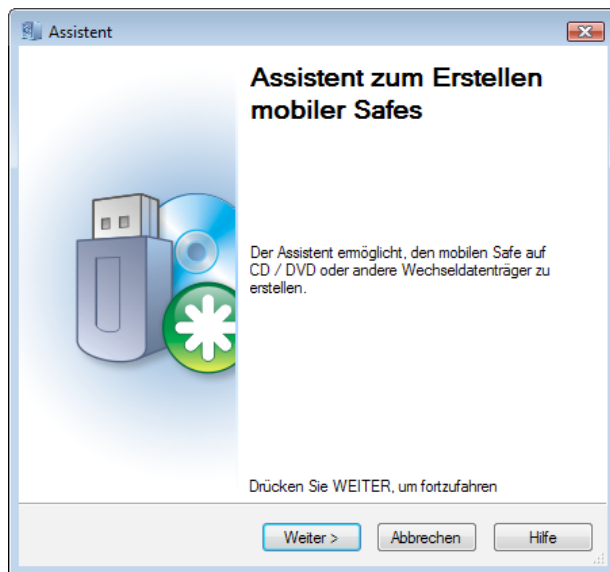
■ Mobiler Safe

TopSecret ermöglicht die Aufnahme des bereits erstellten Safes auf einen Datenträger CD/DVD/USB-Stick, um den Safe außerhalb des Computers zu übertragen. Im Falle der Flash-Speichermedien als auch der wechselbaren Festplatten kann der Safe mit dem jeweiligen Datenträger verknüpft werden. Dank der Option „**Safe mit Datenträger verknüpfen**“ wird es nicht möglich sein, den kopierten bzw. übertragenen Safe auf einem anderen als dem verknüpften Datenträger zu öffnen. Dies stellt eine zusätzliche Sicherheit dar, für den Fall, dass jemand den Safe kopiert. Selbst wenn das geschehen sollte, kann der Datendieb anschließend den Safe auf einem anderen Computer nicht öffnen, denn es ist mit der Festplatte Ihres Computers im übertragenen Sinne „verkettet“ und kann nur auf Ihrem PC geöffnet werden.

Mobilien Safe erstellen

Um den mobilen Safe zu erstellen, loggen Sie sich im Programm als Administrator ein, markieren Sie den Safe und klicken den Button „**Mobilien Safe erstellen**“. Es erscheint ein Willkommensfenster des **Aufnahmeassistenten**. Klicken Sie „**Weiter**“, um zum nächsten Programmschritt zu gelangen.

☐ *Selbstverständlich unterscheidet der Brenn-/Aufnahmeassistent automatisch, ob Sie den Safe auf eine CD/DVD brennen oder auf einen USB-Stick o.ä. kopieren möchten.*



Anschließend erscheint ein Fenster mit Einstellungen der Safeparameter. In diesem Fenster können Sie die Option „**Safe mit Datenträger verknüpfen**“ auswählen, wenn Sie beabsichtigen, den Portablesafe auf einer Wechselfestplatte bzw. einem USB-Stick zu erstellen.

Klicken Sie „**Weiter**“, um ein Medium auszusuchen, auf dem der mobile Safe aufgenommen wird. Das Programm wird automatisch CD/DVD/Flash-Laufwerke sowie mit dem PC verbundene Wechselfplatten erkennen. Wählen Sie aus, ob Sie den mobilen Safe auf einem Wechseldatenträger (also USB-Stick, externe Festplatte, SD-Karte o.ä.) erstellen oder auf einem CD-/DVD-Laufwerk brennen möchten.

Klicken Sie auf „**Weiter**“. Das Programm fragt noch, ob der Dienst „**PKCS#11**“ auf dem Träger aufgenommen werden soll. Dieser Dienst ermöglicht die Anwendung der Zugangsmethoden wie „**Zugang mit Sicherheitszertifikat**“ oder mit biometrischem Lesegerät. Wenn Sie diese Zugangsmethoden auf dem tragbaren Medium nutzen möchten, muss die Option „**Dienst PKCS#11 hinzufügen**“ markiert werden. Klicken Sie auf „**Weiter**“.

Der Safe wird auf dem tragbaren Medium Ihrer Wahl erstellt. Wenn Sie sich entschließen, den Safe auf einer CD/DVD-RW zu erstellen, ist das Programm imstande, die CD/DVD-RW vorher zu löschen. Nach der erfolgten Erstellung können Sie die CD in einen anderen PC einlegen. Selbst wenn das Programm **TopSecret** dort nicht installiert ist, erhalten Sie mit einer der ausgewählten Zugangsmethoden Zugang zu Ihrem Safe.

■ **Mobilen Safe öffnen**

Das Programm **G DATA TopSecret** dient zur Absicherung von sensiblen Daten und nutzt dazu starke Verschlüsselungsalgorithmen. Die Software ermöglicht dem Anwender, seine Daten im virtuellen Safe abzuspeichern, sie sicher auf tragbare Datenträger wie CD/DVD/USB-Sticks, Flash Memory Datenträger, etc. zu überspielen. Wenn Ihnen die notwendigen Passwörter oder Zugangsmethoden (biometrisches Lesegerät oder Zertifikat) zur Verfügung stehen, können Sie ein mit **G DATA TopSecret** verschlüsseltes Verzeichnis auf CD/DVD oder Wechseldatenträger (z.B. USB-Stick) auch auf einem Rechner öffnen und nutzen, auf dem **G DATA TopSecret** nicht installiert ist.

■ *Eine Person, die über entsprechende Berechtigung zum Öffnen des Safes verfügt, ist imstande den Safe auf jedem beliebigen Computer mit dem Betriebssystem **Windows 2000**, **Windows XP** oder **Windows Vista** zu nutzen. Zum Öffnen des mobilen Safes ist es nicht notwendig, die gesamte **G DATA**-Software zu installieren. Neben den Safe-Dateien werden auf dem tragbaren Datenträger sämtliche Softwareelemente abgespeichert, die für die Nutzung des Safes incl. Zugangsmethoden auf einem anderen Computer notwendig sind.*

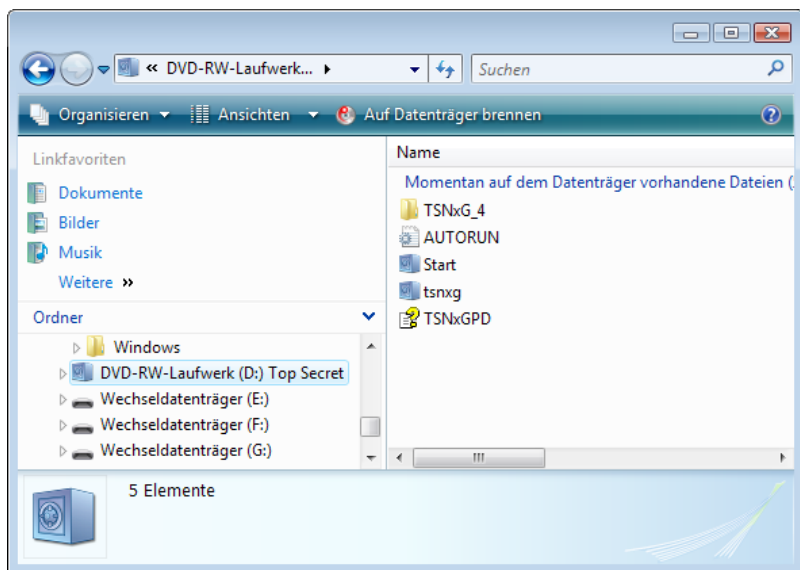
■ **Achtung: Der mobile Safe bietet, wenn er auf einem PC zur Anwendung kommt, auf dem **G DATA TopSecret** nicht installiert ist, keinen Schutzmechanismus gegen das Ausspähen von Passwörtern**

(Keylogger). Diesen Schutz gewährleistet G DATA TopSecret nur, wenn das komplette Programmpaket G DATA NotebookSecurity auf dem jeweiligen Rechner installiert ist.

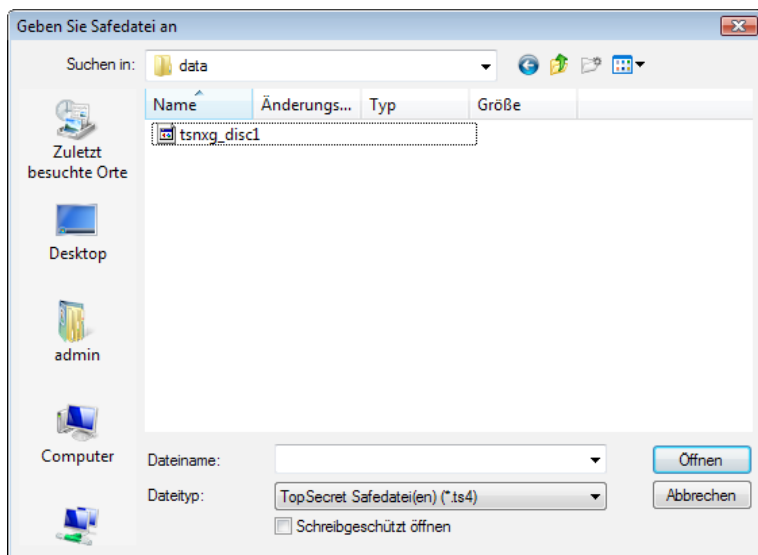
Legen Sie dazu die CD/DVD mit dem Safe in Ihr Laufwerk ein oder verbinden Sie den Wechseldatenträger (z.B. USB-Stick) mit dem Computer. Wenn Sie die Autostart-Funktion Ihres Laufwerks aktiviert haben, öffnet sich eine Dialogbox, in der Sie die Möglichkeit haben, das Programm „Start.EXE“ auszuführen.



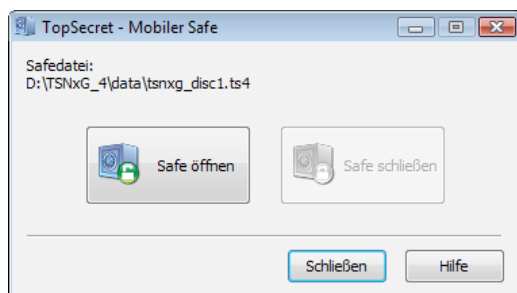
- Sollte die Autostartfunktion nicht aktiviert sein, suchen Sie mit Ihrem Windows-Explorer in Ihrem CD-/DVD-Laufwerk bzw. der Partition des Wechseldatenträgers und klicken dort auf den Eintrag „Start“ bzw. „Start.EXE“.
- **Achtung: Wenn G DATA TopSecret das erste Mal auf einem Rechner genutzt wird, werden nun die entsprechenden Treiberdaten und Programmelemente geladen. Danach ist ein Rechnerneustart notwendig. Nach dem Neustart des Rechners wählen Sie bitte nochmals den Eintrag „Start“ bzw. „Start.EXE“ aus.**



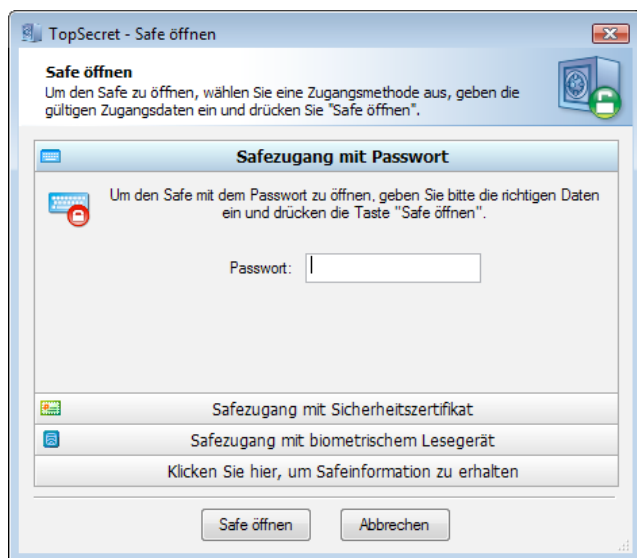
Nun öffnet sich ein Fenster, in dem Sie die Datei auswählen können, welche die Safe-Informationen beinhaltet (z.B. tsnxg_disc1.ts4).



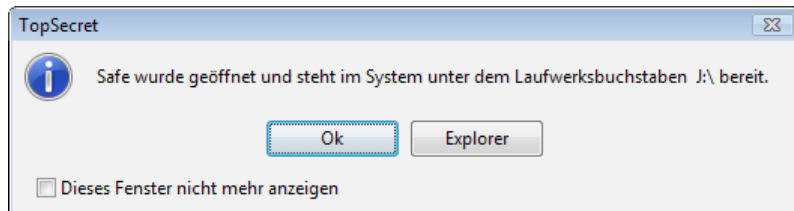
Nun erscheint ein Dialog, mit dem Sie auch auf Rechnern, auf denen **G DATA TopSecret** nicht installiert ist, den Safe öffnen können. Klicken Sie hier auf „Safe öffnen“.



Geben Sie nun Ihr Passwort ein oder nutzen Sie eine der anderen Safezugangsmethoden.



Der Safe wird nun geöffnet und der Inhalt des Safes kann genutzt werden.



Nach dem erfolgten Einloggen in den Safe erscheint im Windows Explorer neben den lokalen Laufwerken das Symbol des Safes als zusätzliches Laufwerk mit einem entsprechenden Laufwerksbuchstaben. Jeder mobile Safebenutzer kann Daten vom Safe auf dem Computer überspielen. Bei Benutzung eines mobilen Safes auf einem USB Datenträger oder FLASH Memory Datenträger kann der entsprechend berechtigte Benutzer die Safedaten von dem Computer in den Safe kopieren.

■ **Achtung: Um Daten auf den mobilen Safe, welcher sich auf einem USB-Stick oder FLASH Memory befindet, kopieren zu können, muss die Safezugangsmethode den vollen Safezugang ermöglichen. Wenn bei der Passwörterstellung die Option „nur zum Lesen“ ausgewählt wurde, wird es dem Anwender nicht möglich sein, Daten in den Safe zu schreiben und dort abzuspeichern.**

Die Safeerstellung und die Nutzung von unterschiedlichen Zugangsmethoden sind im Hauptmenü der Softwarehilfe beschrieben. Das Schließen des mobilen Safes verläuft analog zum Öffnen. Klicken Sie bitte doppelt den Safelaufwerksbuchstaben oder wählen einen entsprechenden Befehl mit der rechten Maustaste im Kontextmenü.

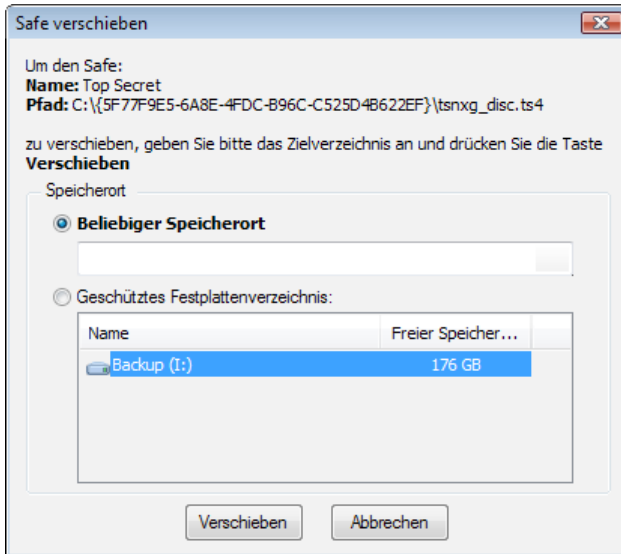
■ **Achtung: Es wird empfohlen, den Safe nach erfolgter Arbeit noch vor dem Herausziehen des tragbaren Datenträgers zu schließen. Gehen Sie dazu auf den tragbaren Datenträger, öffnen das Verzeichnis NotebookSecurity und klicken auf „Start.exe“. Es erscheint dann ein Dialogfenster, in welchem das Schließen des Safes möglich ist.**

■ Bitte beachten Sie, dass Sie an Safe-Inhalten, die sich auf CDs/DVDs befinden, keine Änderungen vornehmen können.

■ Weitere Informationen finden Sie unter: www.gdata.de

■ Safe verschieben

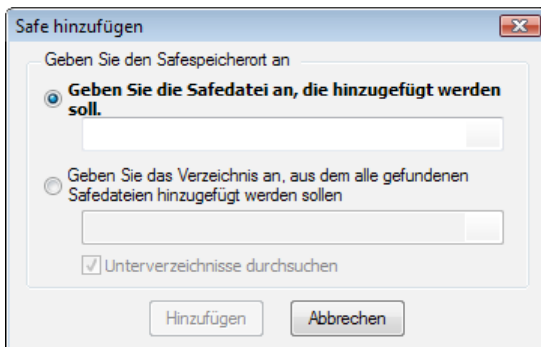
Wenn Sie den Standort Ihres Safes auf der Computerfestplatte ändern möchten markieren Sie den Safe und drücken die Taste „**Safe verschieben**“. Es erscheint ein Fenster, in welchem Sie die erforderlichen Einstellungen vornehmen können. Dabei wählen Sie zwischen der beliebigen Lokalisierung und einer Safelokalisierung auf dem geschützten Festplattenverzeichnis.



Wählen Sie die neue Safelokalisierung aus und drücken die Taste „**Verschieben**“.

■ Safe hinzufügen

Wenn die Notwendigkeit bestand, das Programm **TopSecret** neu zu installieren, wg. System- oder Computerausfalls und auf der Festplatte gibt es bereits früher erstellte Safes, können Sie diese mit Hilfe des Befehls „**Safe hinzufügen**“ vom Programm erkennen und hinzufügen lassen.



Sie können die Safedatei, die hinzugefügt werden soll, direkt eingeben oder ein Verzeichnis auswählen, auf dem sich die Safedateien befinden. Wenn Sie möchten, dass das Programm auch die Unterverzeichnisse mit einschließt, markieren Sie bitte das Feld „**Unterverzeichnisse durchsuchen**“. Klicken Sie anschließend die

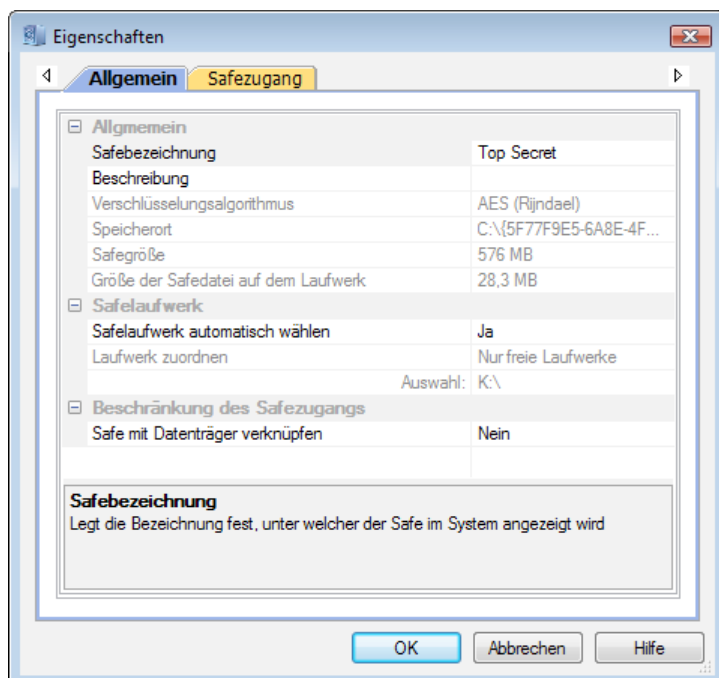
Taste „**Hinzufügen**“. Das Programm erkennt Safes automatisch und fügt sie zu der Safeliste zu.

■ Safe-Eigenschaften

Die Safeeigenschaften können jederzeit verändert werden, nachdem Sie sich als Programadministrator eingeloggt haben. Zu diesem Zweck markieren Sie nach dem Einloggen den gewählten Safe und drücken die Taste „**Safeeigenschaften**“. Das Programm führt anschließend die Authorisierungsprozedur mit einer der vorher definierten Zugangsmethoden durch. In diesem Fall muss die Zugangsmethode gewählt werden, die über Administratorrechte verfügt (siehe Kapitel „Safezugang - Berechtigung“). Nach dem Einloggen in den Safe können manche seiner Einstellungen modifiziert werden.

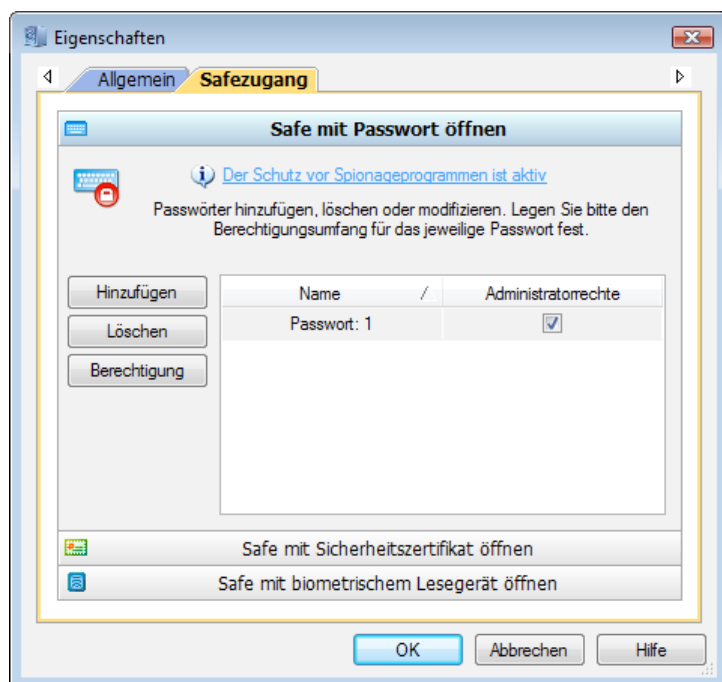
Allgemein

Die Reiterkarte „**Allgemein**“ ermöglicht die Änderung von Safelaufwerksbuchstaben, die im Windows-System sichtbar werden sowie die Verknüpfung des Safes mit dem Datenträger.



Safezugang

Die Reiterkarte „**Safezugang**“ ermöglicht die Änderung von Safeberechtigungen. Hier können die Zugangsmethode (Einloggen), das Passwort und die Berechtigung für das jeweilige Passwort verändert werden.



Die Safezugangsmethoden sind im Kapitel „Safezugang - Einstellung“ beschrieben. Die Berechtigung der jeweiligen Zugangsmethode ist im Kapitel „Safezugang - Berechtigung“ beschrieben.

■ Lizenzvereinbarungen

1. Vertragsgegenstand: Der Lieferant - G DATA Software AG - liefert dem Kunden die Software auf Datenträger. Der Kunde erhält damit das nicht übertragbare Recht, die Vertragssoftware in jedem kompatiblen Computer einzusetzen, vorausgesetzt, dass die Software jeweils nur auf der Anzahl von Computern verwendet wird, welche durch die erworbene Produktvariante lizenziert ist. Der Kunde muss außerdem im Besitz der Original-Software sein. Die Software gilt als in einem Computer eingesetzt, wenn sie in den Direktzugriffsspeicher (d.h. RAM) geladen oder auf einen Festspeicher (wie z. B. Festplatte oder einem anderen Speichermedium) installiert ist. Ferner ist der Kunde dazu berechtigt, von dem erworbenen Produkt genau eine Kopie zum Zwecke der Datensicherung herzustellen. Dabei stellt der Kunde sicher, dass vorhandene Kennungen, Warenzeichen und Urheberrechtsvermerke beim Vervielfältigen unverändert und vollständig übernommen werden. Der Kunde verpflichtet sich, das Produkt sowie die dazugehörige Dokumentation nicht an Dritte weiterzuveräußern; dies gilt nicht für den Fall, dass im Zuge der Übertragung des gesamten Betriebs das Produkt als Teil des Betriebsvermögens an einen Dritten veräußert wird. Der Lieferant liefert das Produkt auf Gefahr und Kosten des Kunden. Der Einsatz der Software in Online-Diensten ist nur mit einer ausdrücklichen Genehmigung der G DATA Software AG zulässig.

2. Bezahlung: Der Rechnungsbetrag ist unverzüglich nach Rechnungseingang ohne Abzug zu leisten. Bis zur vollständigen Entrichtung des Rechnungsbetrags verbleibt das Produkt im Eigentum des Lieferanten.

3. Gewährleistung: Der Lieferant übernimmt die Gewährleistung dafür, dass die überlassene Software verwendbar im Sinne der vorhandenen Programmspezifikation ist. Es wird darauf hingewiesen, dass es nach dem Stand der Technik nicht möglich ist, Fehler in Datenverarbeitungsprogrammen unter allen Anwendungsbedingungen auszuschließen. Für die vollständige Fehlerfreiheit der Programme kann daher keine Gewährleistung übernommen werden. Insbesondere übernimmt der Lieferant keine Gewähr dafür, dass die Programmfunktionen den Anforderungen des Kunden genügen. Voraussetzung für die Gewährleistung ist die vertragsgemäße Nutzung. Bei Mängeln am Datenträgermaterial, die während eines Zeitraums von sechs Monaten dem Lieferanten schriftlich mitgeteilt werden, wird der Datenträger vom Lieferanten ersetzt. Die Gewährleistungsfrist beginnt mit der Übergabe des Programmpakets an den Kunden. Fehler in der Software, also Abweichungen von der festgelegten Programmspezifikation, werden vom Lieferanten beseitigt, sofern die Verwendbarkeit der Software im Sinne der Programmspezifikation erheblich beeinträchtigt ist.

4. Haftung: Für Folgeschäden, die auf die Ergebnisse der Software zurückzuführen sind, wird keinerlei Haftung übernommen.

5. Nebenabreden: Nebenabreden und Vertragsänderungen bedürfen zu ihrer Gültigkeit der Schriftform. Sollte eine der vorstehenden Bestimmungen ganz oder teilweise unwirksam sein, so berührt dies die Wirksamkeit der Bedingungen im übrigen nicht. Der Gerichtsstand für alle Streitigkeiten aus diesem Vertrag ist das zuständige Gericht in Bochum.

■ *Wichtig: Mit Installation der CD erkennt der Kunde diese Allgemeinen Lizenzbedingungen an.*

■ Virengeschichte

Viele "Meilensteine" in der Entwicklung von Viren, Würmern und Trojanern finden Sie in der folgenden Übersicht.

1961: Die Anfänge der Computerviren lassen sich bis 1961 zurückverfolgen. Zu dieser Zeit entwickelten Victor A. Vyssotsky, Robert Morris Sr. und M. Douglas McIlroy auf einem IBM 7090 ein Spiel namens **Darwin**, in dem es darum ging, dass sich selbstgeschriebene Programme auf einem Computer den Speicherplatz streitig machen und gegenseitig löschen. In diesem Zusammenhang wurden auch Programmversionen entwickelt, die sich selber vervielfältigen konnten und hier liegen die eigentlichen Wurzeln der Computerviren. In den 1980er Jahren waren Varianten dieses Spieles als **Core War** unter Programmieren sehr beliebt.

1981: Professor Leonard M. Adleman verwendet im Gespräch mit seinem Doktoranden Fred Cohen zum ersten Mal den Begriff „**Computervirus**“.

1982: Selbstgeschriebene Bootsektorviren für **Apple II Rechner** werden innerhalb eines kleinen Kreises interessierter Programmierer per Diskette ausgetauscht. Der Virus „**Elk Cloner**“ plagt als erster „**in the wild**“-Virus Apple-Nutzer mit Schüttelreimen, invertierten oder falschen Anzeigen und Klickgeräuschen. Er verbreitete sich über Disketten. Als „In the wild“ werden Viren bezeichnet, wenn sie sich tatsächlich unkontrolliert von Rechner zu Rechner verbreiten. Neben „in the wild“-Viren gibt es in Forschungslabors und auf Rechnern von Antivirenspezialisten auch Schadsoftware, die zu Testzwecken entwickelt, aber nie weiterverbreitet wurde.

1983: Im November präsentiert Fred Cohen in einem Seminar das Konzept eines erste funktionsfähigen Virus unter UNIX.

1984: Fred Cohen veröffentlicht erste Artikel über „Experimente mit Computerviren“, die in seine 1986 erschienene Doktorarbeit „Computer Viruses - Theory and Experiments“ einfließen. Seine eher mathematisch ausgerichtete Definition eines Virus ist heute noch anerkannt und umfasst nicht den negativen Beiklang, den der Begriff Virus heute bekommen hat.

1985: Weitere Viren in freier Wildbahn lassen nicht lange auf sich warten. Oft sind es eher Scherzprogramme, die den Computernutzer nur belästigen. Richtig bösar-

tig ist das Trojanische Pferd „**Gotcha**“. Nach dem Start des Programms werden die Daten auf der Festplatte gelöscht und auf dem Bildschirm steht „Arf, arf, Gotcha“.

1986: Die Brüder Basit und Amjad Farooq Alvi betreiben ein kleines Computergeschäft namens „Brain Computer Services“ in Lahore, Pakistan. Um das illegale Kopieren Ihrer Software zu bestrafen, schufen sie einen **Bootsektorvirus** für das Betriebssystem **DOS**. Über pakistanische Studenten verbreitete sich der Virus auch an amerikanischen Hochschulen wie eine Epidemie. Mit „**Virdem**“ wurde der erste **Datei-Virus** freigesetzt und „**PC-Write**“ war das erste **Trojanische Pferd**, dass sich auf Basis eines Shareware-Programmes verbreitete. Viren gerieten durch „**Pakistani-Brain**“ in das öffentliche Interesse. John McAfee und weitere Computerspezialisten gründeten erste Anti-Viren-Firmen.

1987: Immer häufiger erscheinen jetzt Viren, die Dateien befallen. Mit „**Lehigh**“ rückt erstmals ein Virus in das öffentliche Interesse. Lehigh befällt die „command.com“ und nach vier Kopien auf Disketten werden die Daten auf allen im Computer befindlichen Datenträgern gelöscht. Diese radikale Aktion führt allerdings auch zu seiner schnellen Ausrottung. Im Zusammenhang mit „Lehigh“ wird die **VIRUS-L/comp.virus-Mailingliste und -Newsgroup** gegründet und wird zu einer wichtigen Informationsquelle im Kampf gegen Viren. Der „**Cascade-Virus**“ ist der erste verschlüsselte Virus. Der erste Virus für **Amiga** befällt den Bootsektor und gibt ab und an eine Meldung aus. Im Dezember legte ein wohlmeinender amerikanischer Student mit dem ersten Computer-Wurm weltweit den Mailverkehr und die Netzwerke lahm. Der „**Tannenbaum**“-Wurm zeichnet einen Tannenbaum auf den Bildschirm, während er sich im Hintergrund an alle Mailadressen, die er auf dem System finden kann verschickt.

1988: Die wachsende Vernetzung von Computern wird 1988 erstmals von einem neuartigen Schädling ausgenutzt: Dem **Wurm**. Würmer nutzen bis heute Schwachstellen in Netzwerken aus. In dieser Zeit organisierten sich sowohl die Virenautoren als auch die Antiviren-Spezialisten. Antiviren-Software etablierte sich. Der **MacMag Virus** war der erste für **Macintosh** Rechner und hatte eine Reihe weiterer Innovationen zu bieten. Er war der erste Virus, der auf Bestellung (von Chefredakteur des MacMag) entwickelt wurde. Er war auch der erste Virus, der Datendateien befiel, um sich zu verbreiten. Am Freitag dem 13. Mai platzt in Jerusalem zum ersten Mal eine **logische Bombe** (in diesem Fall eine Zeitbombe). Damit war eine neue Virengattung begründet. Robert T. Morris jr. - der Sohn des Computer-Sicherheitsexperten der NSA - setzt einen **Internet Wurm** frei, der sich mit einer kleinen Passwortliste Zugang zu zahlreichen UNIX-Rechnern verschaffte und sich dann wie der Tannenbaum-Virus weiter versendet, was wiederum den Zusammenbruch der Netzwerke und des Mailverkehrs zur Folge hat. Der „Internet-Wurm“ wie er genannt wurde, konnte nur noch durch telefonische Absprachen bekämpft und zur Strecke gebracht werden. Als Reaktion auf die allgemein erhöhte Aktivität der Virenentwickler und speziell den „Internet-Wurm“ wurde in den USA das „**Computer Emergency Response Team /Coordination Center (CERT/CC)**“ gegründet. Es bietet bis heute Rat und Tat rund um den Datenschutz und die Datensicherheit.

1989: Der Virus **DataCrime** verursacht einen riesigen Medienrummel. Mit „**Vienna**“ (**V2Px**) von Mark Washburn erscheinen erste **polymorphe Viren**. Er verschlüsselt sich selbst mit variablen Schlüsseln und ändert auch die Form der Entschlüsselungsroutinen. Er ist deshalb durch Anti-Viren-Software nur mit komplexen Algorithmen aufzuspüren, die zudem zu Fehlalarmen neigten. Das war das Aus für viele Antivirensoftware-Hersteller. Im Juli erscheint die erste Ausgabe des „**Virus Bulletin**“. Seither entwickelte es sich zum renommiertesten Fachmagazin für Virenforscher. In Bulgarien führt **Dark Avenger** zwei Neuheiten ein: 1. Mit dem „**Fast Infector**“ werden nicht nur ausführbare Dateien, sondern auch zum Lesen geöffnete und kopierte Dateien befallen. So ist nach kurzer Zeit die gesamte Festplatte befallen. 2. In unregelmäßigen Abständen werden einzelne Sektoren der Festplatte überschrieben. Das bleibt in den meisten Fällen unbemerkt. **Backups**, die häufig zum Schutz vor Virenbefall angelegt wurden, sind damit wirkungslos. Ein Trojaner wird von der Firma **PC Cyborg** mit Sitz in Panama auf Disketten verteilt, die als AIDS-Information getarnt sind. AIDS ersetzte die autoexec.bat und fing nach einer bestimmten Zahl (90) von Neustarts an die Festplatte zu verschlüsseln. Danach wurde man mit einer Rechnung für den Entschlüsselungscode konfrontiert.

1990: Viren züchten wird jetzt Mode. In **VX (Virus Exchange) Bulletin Boards** werden alte und neue Viren ausgetauscht. **4096 Bytes** ist die Größe des gleichnamigen Virus, der im Januar erscheint. Er hängt sich an ausführbare und geöffnete Datendateien an. Der Mechanismus, der das zu verbergen versuchte führte oft dazu, dass Dateien zerstört wurden. Der Versuch die Nachricht „**Frode Lives**“ anzuzeigen, führte zu einem Systemabsturz. Der Verband deutscher Virenliebhaber verbreitet das erste **Virus Construction Kit für DOS**. Damit ist es auch Anfängern möglich, Viren nach Maß zu erstellen. Im Dezember wird das **European Institute for Computer Antivirus Research** (kurz **EICAR**) gegründet. Es spielt bis heute eine wichtige Rolle im Kampf gegen Viren und Virenautoren.

1991: **Michelangelo** ist ein Bootsektor-Virus, der am 6. März - dem Geburtstag Michelangelos - die ersten 256 Sektoren des Datenträgers überschreibt. Damit wird der Rechner unbrauchbar. Im darauffolgenden Jahr wird Michelangelo in den Medien breit getreten, was sicher etlichen Schaden verhindert hat. Er ist trotzdem noch lange Jahre aktiv. **Polymorphe Viren** werden jetzt immer häufiger. **Tequila** ist der erste weit verbreitete polymorphe Virus. **Maltese Amoeba** überschreibt an zwei bestimmten Tagen des Jahres den ersten Sektor des Datenträgers. Robert Slade beginnt seine Reihe mit Computer-Viren-Tutorials. Kurz darauf beginnt er mit den Arbeiten am **VIRUS-L-FAQ**. Der „**Saddam-Hussein**“-Virus verschlüsselt auf Amiga-Rechnern Teile des Datenträgers, so dass diese nur noch gelesen werden können, wenn der Virus im Speicher ist.

1992: Der **Commodore Amiga** und der **Atari ST** verlieren ihre Bedeutung und **MS-DOS** setzt sich immer mehr durch. Entsprechend steigt die Anzahl der **DOS-Viren**. **Altair** für Atari ST gibt sich als Antiviren Software aus. Er überschreibt alle Viren, die er im Bootsektor findet. Er scheitert wie viele andere „**Antiviren-Viren**“. Ein Virenautor, der sich **Dark Avenger** nennt, veröffentlicht die **Self Mutating Engine**

(**MtE**). Damit lassen sich aus normalen Viren mit wenig Aufwand polymorphe Viren erzeugen. **MtE** ist damit das erste **Toolkit** zur Erzeugung von polymorphen Viren. Ebenfalls von Dark Avenger stammt **Commander Bomber**, der einen neuen Tarnmechanismus verwendet. Er befällt COM-Dateien, hängt sich aber nicht in einem Block an die Datei, sondern verteilt seinen Code auf mehrere Fragmente, die untereinander durch Links verbunden sind. Um ihn zu erkennen, muss die gesamte Datei gescannt werden.

1993: Neue Toolkits zur Erzeugung von polymorphen Viren erscheinen: **Trident Polymorphic Engine (TPE)**, **Nuke Encryption Device (NED)** und **Dark Angel's Multiple Encryption (DAME)** bauen auf der MtE auf. **Virensignaturen** werden aber weiterhin verwendet. In MS-DOS 6 ist erstmal ein (mittelmäßiger) Virens Scanner enthalten. Der Amiga-Virus **Fuck**, der durch einen als Modem-Testprogramm getarnten Trojaner verbreitet wurde, ersetzte zunächst die Systemdatei loadWB. Nach einem Neustart des Rechners wurde der Virencode ausgeführt: Nach einer bestimmten Zeit, die durch die Bildwiederholfrequenz festgelegt war, wurde die gesamte Festplatte mit dem bösen F-Wort voll geschrieben, was zur Zerstörung aller Daten führte. Joe Wells veröffentlicht die erste **Wildlist**. Er möchte damit die Aktivitäten von Viren auflisten, die im Umlauf sind. Aus dieser Liste ist später die **Wildlist Organization** entstanden. Erste Computerviren für **Windows** tauchen auf.

1994: Die ersten **Multipartite-Viren** tauchen auf. Diese Viren nutzen mehrere Infektionsmechanismen und können gleichzeitig neben Dateien auch Bootsektoren bzw. Partitionstabellen befallen. Black Baron veröffentlicht **Smeg.Pathogen** (und **Smeg.Queen**). Smeg.Pathogen zeigt eine Meldung an und überschreibt anschließend die ersten 256 Sektoren der Festplatte. Das hat in einigen Firmen zu erheblichen Schäden geführt. Er wurde im darauf folgenden Jahr zu einer Gefängnisstrafe verurteilt. **Kaos4** verbreitete sich über eine **Newsgroup**, die auf Erotikbilder spezialisiert war. Diese Strategie wurde seitdem häufiger angewandt. **Virus Hoaxes** (= Warnungen vor Viren oder anderen Schadprogrammen, die gar nicht existieren) werden mit den „**Good-Times**“-Warnungen zu einem ernsthaften aber verkannten Problem.

1995: 1995 tauchen mit „**DMV**“ und „**Nachtwächter**“ die ersten **Makroviren** auf. Bis dahin wurden nur ausführbare Dateien und Bootsektoren befallen. **Melissa**, **Loveletter**, **Sobig** und Konsorten stellen immer wieder neue Geschwindigkeitsrekorde bei der Verbreitung auf. „**Concept 1995**“ war der erste Makrovirus der öffentlich ausbrach und sich ungehindert in englischen Systemen verbreitete. Mit **Hunter.c** erscheint der erste polymorphe Makrovirus in Deutschland. **Wm.Concept** war der erste „in the wild“ Makrovirus. Er enthielt nur die Meldung „That's enough to prove a point.“ (etwa: „das reicht als Beweis“) und war kurze Zeit später der weltweit verbreitetste Virus. Wm.Concept begründete die Gattung der „**Proof of Concept**“-Viren. PoC-Viren zeigen nur, dass es möglich ist eine bestimmte Schwachstelle auszunutzen, ohne wirklich Schaden anzurichten. Die Erkennung von Makroviren stellt hohe Anforderungen an die Virens Scanner, nicht zuletzt wegen der ständig wechselnden Formate von Skriptsprachen und Office-Dateien.

1996: Es erscheinen erste **Makro-Generatoren** für deutsche oder englische Makroviren. Makroviren beschränken sich nicht länger auf **Word**, sondern zielen auch auf **Excel** und **AmiPro** Dateien ab. Sie überspringen auch die Grenzen zwischen Betriebssystemen und befallen sowohl PCs als auch Macs. **Laroux** infiziert als erster MS-Excel-Dateien. **Boza** befällt als erster Virus das PE-EXE-Format von Windows 95-Dateien.

1997: Viren werden jetzt immer spezieller und greifen gezielt Schwachstellen in Programmen, Betriebssystemen oder Hardware an. Das erste Virus für das Betriebssystem **Linux** taucht auf.

1998: Strange Brew ist der erste Virus für **Java**. Abgesehen von Makroviren waren PCs mit **MacOS** seit mindestens drei Jahren nicht von Viren geplagt. Mit dem Wurm **Autostart.9805** ändert sich das. Autostart nutzt den Quicktime AutoStart Mechanismus auf PowerPCs und kopiert sich auf Festplatten und andere Datenträger. Bestimmte Dateien werden mit Datenmüll überschrieben und damit unbrauchbar gemacht. AutoStart verbreitet sich von HongKong über die ganze Welt. **CIH (Spacefiller, Chernobyl)** hat eine der massivsten **Payloads** (= Schadteil eines Virus). Er belebt die Frage, ob Viren in der Lage sind, Hardware zu zerstören. Wenn seine Schadensfunktion (am 26. eines Monats) aktiv wird, überschreibt er das **Flash-BIOS** und die Partitionstabelle der Festplatte. Damit lässt sich der Rechner nicht mehr booten. Auf einigen Motherboards mussten die BIOS-Bausteine ausgetauscht oder neu programmiert werden. Aber selbst nach der Wiederherstellung des Systems waren die Daten verloren.

1999: Im Zusammenhang mit **Back Orifice** wird diskutiert, ob es eine Fernwartungs- oder eine Fernsteuerungs-Software ist. Da die Fernsteuerungs-Funktionen ohne Wissen des Nutzers ausgeführt werden können, ist Back Orifice als **Trojaner** zu bezeichnen. Mit Back Orifice gelingt einem Angreifer Mitte 2000 ein Einbruch ins interne Firmennetz von Microsoft. Im März befällt der Wurm „**Melissa**“ bereits am ersten Tag seines Erscheinens zigtausende Computer und verbreitet sich in Windeseile weltweit. Er versendet E-Mails an die ersten 50 Adressen im Adressbuch und die befallenen Rechner brechen unter der Last eingehender E-Mails zusammen. **Happy99** erzeugt von jeder vom Nutzer versendeten Mail eine Kopie und verschickt sie erneut mit dem gleichen Text und der gleichen Betreffzeile plus dem Wurm im Dateianhang. Das funktioniert auch bei **Usenet**-Postings. Abgesehen von E-Mail verbreitet sich **Pretty Park** auch über **Internet Relay Chats (IRC)**. Er hat sehr effektive Schutz- und Tarnmechanismen, die verhindern, dass der Wurm gelöscht werden kann. Beim nächsten Virenskan wird der Wurm als legitim erkannt. Manchmal werde Virenskan auch blockiert. Für Nutzer von Outlook wird mit **Bubbleboy** die „Good-Times“ Vision wahr, dass ein Virus den Rechner allein schon dadurch infiziert, dass man eine E-Mail liest. **ExploreZip** tarnt sich als sich selbst entpackendes Archiv, das als Antwort auf eine eingegangene E-Mail gesendet wird. Er verbreitet sich über Netzwerkfreigaben und kann einen Rechner auch dann infizieren, wenn ein anderer Nutzer unvorsichtig ist. Die Schadensfunktion durchsucht die Festplatte nach C und C++ Programmen, Excel-, Word- und Powerpoint-Dateien und löscht sie.

2000: Trotz aller Prophezeiungen gibt es keinen **Millenium-Wurm**, der diesen Namen verdient hätte. **Palm/Phage** und **Palm/Liberty-A** sind zwar selten aber durchaus in der Lage **PDAs** mit **PalmOS** zu befallen. Der **VB-Skript-Wurm VBS/KAKworm** nutzt eine Schwachstelle in Scriptlets und Typelibs des Internet Explorers. Ähnlich wie **BubbleBoy** verbreitete er sich beim Öffnen einer E-Mail (auch in der Voransicht). Im Mai versendet ein Wurm lawinenartig E-Mails aus dem Outlook-Adressbuch mit der Betreffzeile „**I love you**“ und richtet vor allem in großen Unternehmens-Netzen Milliarden Schäden an. Auch hier sind die Netze binnen Kurzem völlig überlastet. Von der Urfassung eines philippinischen Studenten namens Onel de Guzman werden zahlreiche Varianten abgeleitet. US-Experten sprechen vom bösartigsten Virus der Computergeschichte. Nach dem **Loveletter** und seinen vielen Varianten wurden an den MailGateways einfach die Mails mit den entsprechenden Betreffzeilen herausgefiltert. **Stages of Life** variierte die Betreffzeile und schlüpfte so durch die Maschen. Der Autor von **W95/MTX** hat sich alle Mühe gegeben, um den Wurm/Virus-Hybriden vom Rechner zu entfernen. Er versendete eine PIF Datei mit doppelter Dateiendung per E-Mail. Er sperrt den Zugriff des Browsers auf einige Websites von Antiviren-Herstellern, versucht Dateien mit der Viruskomponente und einige Dateien werden durch die Wurmkomponente ersetzt.

2001: Code Red nutzt einen **Bufferoverflow-Fehler** in der **Internet Information Server (IIS) Indexing Service DLL** von Windows NT, 2000 und XP. Er scant zufällig IP Adressen auf dem Standardport für Internetverbindungen und überträgt einen Trojaner, der zwischen dem 20. und 27. eines Monats eine **Denial of Service (DoS) Attacke** gegen die Webseite des Weißen Hauses startet. Die Entfernung des Virus ist sehr aufwändig und verschlingt Milliarden.

2002: Der Wurm „**MyParty**“ zeigt Anfang des Jahres, dass nicht alles, was mit „.com“ endet eine Webseite ist. Wer den Mailanhang „www.myparty.yahoo.com“ doppelklickt bekommt anstelle der erwarteten Bilder einen Wurm mit Backdoor-Komponente. Im Frühjahr und Sommer nutzt **Klez** die IFRAME-Sicherheitslücke im Internet Explorer um sich automatisch beim Betrachten einer Mail zu installieren. Er verbreitet sich per E-Mail und Netzwerk und hängt sich an ausführbare Dateien. Am 13. von geraden Monaten (in späteren Versionen waren es andere Tage) werden alle Dateien auf allen erreichbaren Laufwerken mit zufälligen Inhalten überschrieben. Die Inhalte lassen sich nur durch Backups wiederherstellen. Im Mai verbreitet sich **Benjamin** als erster Wurm über das **KaZaA-Netzwerk**. Er kopiert sich unter vielen verschiedenen Namen in einen Netzwerkordner. Auf infizierten Rechnern wird eine Webseite mit Werbung angezeigt. Zuvor waren auch **Gnutella** basierte **P2P Netzwerke** befallen. **Lentin** ist ein Wurm, der es ausnutzt, dass viele Leute nicht wissen, dass **SCR-Dateien** nicht nur einfache Bildschirmschoner, sondern auch ausführbare Dateien sind. Verglichen mit Klez ist sein Videoeffekt als Schadensfunktion nur störend. Auch seine Verbreitung erreicht nicht die von Klez. Ende September verbreitet sich **Opasoft** (auch **Brazil** genannt) wie eine Epidemie. Auf Port 137 scant er Rechner im Netzwerk und prüft, ob es dort Datei- und/oder Drucker-Freigaben gibt. Dann versucht er sich auf den Rechner zu kopieren. Wenn

es einen Passwortschutz gibt, wird eine Liste mit Passwörtern durchlaufen und eine Schwachstelle in der Speicherung von Passwörtern ausnutzt. **Tanatos** alias **BugBear** ist der erste Wurm, der Klez seit dem Frühjahr von seinem Spitzenplatz verdrängt. Der Wurm verbreitet sich per E-Mail und Netzwerk, installiert eine **Spyware-Komponente** und versendet Aufzeichnungen der Tastaturanschläge.

2003: Im Januar legt „**W32/SQL-Slammer**“ für Stunden das Internet lahm, weil er eine Schwachstelle im **Microsoft SQL-Server** ausnutzt, um Datenbankinhalte zu versenden. Der Massenmailwurm „**Sobig.F**“ stellt mit seiner eigenen Mailengine einen neuen Rekord für die Verbreitungsgeschwindigkeit auf. Er verbreitet sich zehn Mal schneller als bisherige Würmer.

2004: Rugrat ist der erste Virus für 64-bit Windows. Cabir, der erste Virus für **Mobiltelefone** mit **Symbian** Betriebssystem und **Bluetooth** Schnittstelle wird von der für ihre Proof-of-Concept-Viren bekannte Gruppe **29A** entwickelt. Kurz darauf folgt von der gleichen Gruppe mit **WinCE4Dust.A** der erste **PoC-Virus** für **Windows CE**.

2005: Als erster Wurm für **Symbian Smartphones** verbreitet sich **CommWarrior.A** per **MMS**. Die MMS-Nachrichten werden von variablen begleitenden Texten als Antiviren-Software, Spiele, Treiber, Emulatoren, 3D Software oder interessante Bilder dargestellt und an alle Einträge des Telefonbuchs versendet.

2006: In diesem Jahr versucht der Schallplattenkonzern Sony BMG mit einer Installation von **Rootkit-Software** auf seinen Audio-CDs, ein Kopieren dieser CDs zu verhindern. Abgesehen von der Diskussion über Sinn, Zweck und Imageschaden dieser Aktion rückt das RootKit in den Focus der Virenentwickler und immer mehr RootKits mit Backdoor-, Trojaner- und Schadfunktionen überschwemmen den Markt. Einmal installierte Rootkits sind selbst für moderne Antivirenprogramme schwer zu erkennen.

2007: Neben **Phishing**- und **Pharming**-Attacken, bei denen versucht wird, Anwender sensible Informationen (wie z.B. **Onlinebanking-Daten**) zu entlocken, werden die Schreiber von Schadsoftware auch in anderer Hinsicht zunehmend geschäftstüchtig. Über **BotNetze** werden viele Computer argloser Anwender ferngesteuert (Stichwort: **Zombie-PC**) und für Spam-Mails oder gezielte Attacken auf die Internet-Infrastruktur verwendet.

■ Glossar

Abgesicherter Modus: Nach einem Systemabsturz startet Windows automatisch im „Abgesicherten Modus“. Dabei werden nur die unbedingt benötigten Systemdateien und Treiber geladen. So lassen sich Änderungen am System vornehmen, die im normalen Betrieb nicht möglich wären. Dies kann man auch dazu nutzen, um fehlerhafte Programme oder Viren, Würmer und Trojaner zu beseitigen.

Account: Als Account bezeichnet man die Zugangsberechtigung zu einem Computersystem. Dieser untergliedert sich in der Regel in eine Benutzerkennung (User-Identification) und ein geheimes Passwort.

Active Scripting: Eine der ursprünglichen Stärken des Internet Explorers sind die umfassenden Möglichkeiten aktive (d.h. ausführbare) Inhalte darzustellen. Um dies zu gewährleisten, unterstützt der Internet Explorer die Ausführung von Java Applets, ActiveX Controls und Skriptsprachen wie JavaScript, VBScript etc. Neuerdings gehören auch .NET Komponenten dazu. Leider bieten aktive Inhalte nicht nur Vorteile. Immer wieder nutzen Anbieter von Webseiten die Möglichkeiten, um Ihre Besucher auszuspionieren. Auch Viren, Würmer und Trojaner verbreiten sich auf diesem Weg. Daher wird häufig empfohlen aktive Inhalte zu deaktivieren. In den Sicherheitseinstellungen des Internet Explorers (Menüleiste: Extras oder Ansicht > Internetoptionen oder Optionen > Sicherheit > Stufe anpassen) lassen sich diese Komponenten für die verschiedenen Zonen ein- oder ausschalten. Mehr dazu erfahren Sie bei Microsoft.

Active Server Pages: Active Server Pages ist eine von Microsoft entwickelte WebServer Technologie, die HTML-Seiten aus Datenbanken dynamisch generieren kann.

ActiveX: ActiveX bezeichnet eine Technologie, die auf dem Component Object Model (COM) von Microsoft beruht. Sie ermöglicht es Softwarekomponenten, miteinander zu interagieren, auch wenn sie von unterschiedlichen Personen, zu unterschiedlichen Zeiten, mit unterschiedlichen Tools in unterschiedlichen Programmiersprachen geschrieben wurden. Die Komponenten - auch ActiveX Steuerelemente (engl. ActiveX Controls) genannt - müssen noch nicht einmal auf dem gleichen Rechner vorhanden sein. Durch ihren modularen Charakter lassen sich ActiveX Controls einfach in eigene Programme einbinden. Der Programmierer muss dazu lediglich die Spezifikation der Schnittstelle kennen. Nicht nur in Anwendungen von Microsoft werden ActiveX Controls eingesetzt. Sie werden z.B. dafür verwendet, um Word-, Excel- oder PowerPoint-Dokumente im Internet Explorer zu öffnen. Man spricht dann von ActiveX Dokumenten.

Administrator: Administrator ist die Bezeichnung für den Systemverwalter eines Netzwerks, der uneingeschränkte Zugriffsrechte hat und für die Betreuung und Verwaltung des Netzwerks zuständig ist.

Aktiver Inhalt: Eine der ursprünglichen Stärken des Internet Explorers sind die umfassenden Möglichkeiten aktive (d.h. ausführbare) Inhalte darzustellen. Um dies zu gewährleisten, unterstützt der Internet Explorer die Ausführung von Java Applets, ActiveX Controls und Skriptsprachen wie JavaScript, VBScript etc. Neuerdings gehören auch .NET Komponenten dazu. Leider bieten aktive Inhalte nicht nur Vorteile. Immer wieder nutzen Anbieter von Webseiten die Möglichkeiten, um Ihre Besucher auszuspionieren. Auch Viren, Würmer und Trojaner verbreiten sich auf diesem Weg. Daher wird häufig empfohlen aktive Inhalte zu deaktivieren. In den Sicherheitseinstellungen des Internet Explorers (Menüleiste: Extras oder Ansicht > Internetoptionen oder Optionen > Sicherheit > Stufe anpassen) lassen sich diese Komponenten für die verschiedenen Zonen ein- oder ausschalten. Mehr dazu erfahren Sie bei Microsoft.

American National Standards Institute: Das „American National Standards Institute“ befasst sich mit Standardisierungen und hat z.B. den ASCII-Standard entwickelt.

American Standard Code for Information Interchange: Der „American Standard Code for Information Interchange“ ist der weltweit geltende Standard um Buchstaben, Ziffern und Sonderzeichen in Byte zu kodieren.

API: Das „Application Programming Interface“ ist eine standardisierte Schnittstelle, über die ein Programm auf ein anderes Programm oder Peripheriegeräte zugreifen kann.

Applet: Ein Applet ist eine Softwarekomponente, die nicht eigenständig benutzt wird, sondern das Leistungsspektrum eines Programms ergänzt. Auch Java-Programme werden als Applets bezeichnet, wenn sie in einem Browser ausgeführt werden.

Application Programming Interface: Das „Application Programming Interface“ ist eine standardisierte Schnittstelle, über die ein Programm auf ein anderes Programm oder Peripheriegeräte zugreifen kann.

Archiv: In einem Archiv sind mehrere Dateien und Verzeichnisse in eine Datei zusammengefasst. Um Festplattenspeicherplatz zu sparen oder Daten schneller zu versenden, können Sie diese mit diversen Packprogrammen (z.B. Winzip, WinRAR) je nach Datentyp auf ein erheblich geringeres Maß komprimieren. Diese Dateien haben Endungen wie z.B. „.zip“, „.rar“ oder „.arj“ und können in der Regel erst nach dem Entpacken durch das jeweilige Packprogramm von anderen Anwendungen wieder genutzt werden. Der Zugriff auf ein Archiv kann mittels eines Passwortes eingeschränkt werden.

ASCII: Der „American Standard Code for Information Interchange“ ist der weltweit geltende Standard um Buchstaben, Ziffern und Sonderzeichen in Byte zu kodieren.

ASP: Active Server Pages ist eine von Microsoft entwickelte WebServer Technologie, die HTML-Seiten aus Datenbanken dynamisch generieren kann.

AT-Befehle: Über AT-Befehle können ISDN-Karten und Modems angesprochen und gesteuert werden.

Attachment: Attachment ist die englische Bezeichnung für eine Datei, die an eine E-Mail angehängt wurde.

Auslagerungsdatei: Jeder Rechner enthält einen Speicherbereich, in dem die Daten, die gerade vom Rechner gebraucht werden abgelegt werden. Diesen Bereich nennt man RAM (Random Access Memory). Der Zugriff auf den RAM-Speicher ist viel schneller als der Zugriff auf die Festplatte. Die Größe des RAMs ist allerdings beschränkt (z.B. auf 256 MB). Wenn jetzt sehr viele und/oder große Dateien geöffnet sind, kann es vorkommen, dass nicht alle Dateien im RAM Platz haben. Dann wird ein Teil des RAMs auf die Festplatte ausgelagert - und zwar in die Auslagerungsdatei.

BootScan: Der BootScan prüft vor der Installation des Virenschutzprogramms, ob Ihr System bereits von Viren befallen ist. Falls Sie versäumen, den BootScan durchzuführen, kann es Ihnen passieren, dass Stealth-Viren den Virenschutz umgehen und erst später oder gar nicht auffallen.

BCC: Mit einer ‚Blind Carbon Copy‘ (bcc) können E-Mails an mehrere Empfänger versandt werden, ohne dass die Adressaten die E-Mail-Adressen der anderen Empfänger mitgeteilt bekommen.

BIOS: Das Basic Input Output System ist die erste Software, die nach dem Einschalten eines Computers geladen wird. Es führt beim Einschalten einen Selbsttest durch (POST = Power On Self Test), initialisiert die Hardware und lädt den Code aus dem ersten Sektor (Master Boot Record MBR) eines Datenträgers. Es umfasst zusätzlich Ein-/ und Ausgaberoutinen für Hardware, auf die das Betriebssystem zugreift. Da es von der Hardware abhängig ist, kann das BIOS nicht beliebig ausgetauscht werden. Das BIOS ist auf einem speziellen Chip auf dem Motherboard gespeichert, wo diese Daten auch erhalten bleiben, wenn die Stromzufuhr unterbrochen ist. Auf vielen Computern kann das BIOS mit Hilfe von Software des BIOS- Herstellers aktualisiert werden. Es kann auch von Viren, wie W95/CIH-10xx beschädigt werden, so dass der PC nicht mehr booten kann. Wenn der BIOS-Chip nicht ersetzt werden kann (einige BIOS-Chips sind verlötet), muss sogar das Motherboard des Computers ausgetauscht werden.

Bit: Abkürzung für „Binary digIT“. Ein Bit ist die kleinste Informationseinheit in der Computertechnik und kann die Werte 0 oder 1 annehmen.

Blind Carbon Copy: Mit einer ‚Blind Carbon Copy‘ (bcc) können E-Mails an mehrere Empfänger versandt werden, ohne dass die Adressaten die E-Mail-Adressen der anderen Empfänger mitgeteilt bekommen.

Bluetooth: Bluetooth ermöglicht die Kommunikation zwischen Computern, PDAs, Mobiltelefonen und Peripheriegeräten wie Tastatur oder Maus. 1994 begann die Entwicklung der Schnittstelle bei Ericsson. Mittlerweile ist Bluetooth als IEEE Standard 802.15.1 für drahtlose Vernetzung über kurze Entfernungen etabliert. Der Name Bluetooth ist von dem dänischen König Harald I. Blauzahn Gormson abgeleitet, dem es im zehnten Jahrhundert gelang die skandinavischen Völker zu einen. Analog sollte Bluetooth zu einer Einigung bei der Kommunikation von elektronischen Kleingeräten führen. Technisch basiert Bluetooth auf einem kostengünstigen und stromsparenden Mikrochip das im ISM-Band zwischen 2,402 GHz und 2,480 GHz sendet - und zwar weltweit und lizenzfrei.

Bookmark: Über Bookmarks (= Lesezeichen) konnte man ursprünglich in einem Web-Browser interessante Internet-Adressen speichern. Die Favoriten - wie die Bookmarks bei Microsoft heißen - können zusätzlich in Word, Excel, PowerPoint, Outlook und anderen MS-Programmen auf interessante Objekte verweisen.

Boot Record: Dieser Eintrag enthält Informationen zum Inhalt einer Diskette oder HardDisk und Informationen, die ein Rechner braucht, um von diesem Medium zu booten. Auf den Boot Record wird vom Bootsektor aus verwiesen.

Bootsektor: Der Bereich auf einer Diskette oder einem Laufwerk, der den Boot Record enthält.

Browser Hijacker: Browser Hijacker installieren sich unbemerkt und ändern Einstellungen des Browsers (z.B. die Startseite) und dessen Funktionen (z.B. Suchfunktion). Daher gehören sie eigentlich zu den Trojanern. Browser Hijacker leiten den Nutzer ungewollt auf (oft pornografische) Webseiten indem die Startseite oder die Suchfunktion umgeleitet wird. Manchmal werden auch zusätzliche Menüleisten oder

Fenster angezeigt, die sich nicht entfernen oder schließen lassen. Oft nutzen Browser Hijacker Sicherheitslücken und Schwachstellen des Systems, um sich tief darin einzunisten. Meist wird der Internet Explorer angegriffen. Die Beseitigung der Fehlfunktionen ist oft sehr umständlich. Einer der berüchtigtsten Browser Hijacker ist CoolWeb.

Brute-Force Angriff: ein Brute-Force Angriff ist eine Möglichkeit, um Passwörter von verschlüsselten Dateien zu knacken. Dabei probiert man alle möglichen Kombinationen aus. Mit schnellen Rechnern und schwacher Verschlüsselung oder schwachen Passwörtern funktioniert das. Bei den aktuellen Sicherheitsstandards sind die Chancen für Brute-Force Angriffe aber äußerst gering.

Buffer Overflow: Bei einem Buffer Overflow überflutet ein Angreifer Datenfelder mit einer zu großen Datenmenge. Unter Umständen ist es so möglich, im Speicher der Rechners eigenen Programmcode auszuführen und versteckte Befehle zu übermitteln, die dem Angreifer einen Zugang auf diesen Rechner ermöglichen.

Bug: Der Begriff stammt aus den Zeiten als Rechnern noch mit Relais betrieben wurden. Hier sorgten Käfer (engl. Bug) für Programmfehler. Als Bug bezeichnet man seither einen Fehler in einem Software-Programm. Die meisten Hersteller bieten in so einem Fall einen sogenannten Patch an, der den Fehler behebt.

Bulk Mail: Bulk Mail steht für Massenpost. Der Begriff ist eine etwas mildere Bezeichnung für Spam.

Button: Button (engl.: Knopf) bezeichnet die oft stilisiert dargestellten Eingabetasten, die in Programmen und Internetseiten verwendet werden. Bewegen Sie die Maustaste über den Button und klicken Sie mit der linken Maustaste einfach oder doppelt auf den Knopf um die dort hinterlegten Funktionen auszuführen.

Byte: Ein Byte sind 8 Bit.

Cache: Der Cache ist eine schneller Zwischenspeicher, der dafür sorgt, dass oft abgerufene Daten nicht ständig neu übertragen werden müssen.

Carbon Copy: Per „Carbon Copy“ können beliebig viele Kopien einer E-Mail an weitere Empfänger verschickt werden. Die Nachricht muss dazu nur einmal geschrieben und versendet werden.

Carrier: Modem-Trägersignal zur Erkennung von Sender und Empfänger.

Cascading Style Sheet: Mit „Cascading Style Sheets“ können Formatvorlagen für Internetseiten definiert werden.

CC: Per „Carbon Copy“ können beliebig viele Kopien einer E-Mail an weitere Empfänger verschickt werden. Die Nachricht muss dazu nur einmal geschrieben und versendet werden.

CGI: Das „Common Gateway Interface“ ermöglicht einem Web-Browser, auf einen Web-Server Programme auszuführen. Sogenannte CGI-Scripts können dabei z.B. HTML-Formulare auswerten oder Datenbankabfragen durchführen.

Client: Client-Programme empfangen Daten von einem Server. Ein Computer wird dann Client genannt, wenn er auf diese Weise Daten von einem Server empfängt. Web-Browser sind z.B. klassische Client-Programme.

Common Gateway Interface: Das „Common Gateway Interface“ ermöglicht einem Web-Browser, auf einen Web-Server Programme auszuführen. Sogenannte CGI-Scripts können dabei z.B. HTML-Formulare auswerten oder Datenbankabfragen durchführen.

Companion Virus: Wenn sich zwei ausführbare MS-DOS Programme nur im Dateityp (also der Dateiendung) unterscheiden, wird das mit der Endung .COM vor dem mit der Endung .EXE ausgeführt. Diese Eigenschaft machen sich Companion-Viren zu Nutze. Z.B. könnte ein Companion Virus sich unter dem Namen „DIR.COM“ in das DOS-Verzeichnis kopieren. Wenn dann ein Anwender den Inhalt eines Verzeichnisses anzeigen möchte, wird der Virus aufgerufen und nicht das gewünschte Programm „DIR.EXE“.

Compiler: Compiler übersetzen Programmiersprachen in einen Maschinencode, der vom Rechner verarbeitet werden kann.

Cracker: Cracker sehen Ihre Lebensaufgabe darin, den Kopierschutz von Software durch sogenannte Cracks oder das Herausfinden von Seriennummern zu umgehen. Zu den Crackern zählen auch Personen, die das Datennetz dazu missbrauchen, sich Zugriff auf fremde Rechner zu verschaffen, um sich persönlich zu bereichern oder einfach nur Schaden anzurichten.

CRC: Der „Cyclic Redundance Check“ ist ein Prüfsummenverfahren, mit dem festgestellt werden kann, ob Datenpakete fehlerfrei übertragen wurden.

Cross Site Scripting: Eine Sicherheitslücke, bei der Skripte von einer Webseite in einer anderen Webseite ausgeführt werden. Der Nutzer merkt nicht, dass ein fremdes Skript ausgeführt wird, da sich die angezeigte URL-Adresse nicht ändert.

CSS: Mit „Cascading Style Sheets“ können Formatvorlagen für Internetseiten definiert werden.

Cyberspace: Der Autor William Gibson verwendete 1984 in seinem „Cyber-Thriller“ „Neuromancer“ das erste Mal den Ausdruck „Cyberspace“ und bezeichnete damit den virtuellen Raum eines globalen Computernetzwerks.

Cyclic Redundancy Check: Der „Cyclic Redundance Check“ ist ein Prüfsummenverfahren, mit dem festgestellt werden kann, ob Datenpakete fehlerfrei übertragen wurden.

Daemon: Der „Disk And Execution MONitor“ ist ein Programm, das im Hintergrund eines Netzwerks auf bestimmte Ereignisse wartet und bei Eintritt eines solchen Ereignisses bestimmte Aktionen startet. So wartet ein Mailer Daemon etwa auf eingehende E-Mails und ein Spooler wartet auf Druckaufträge.

Data Encryption Standard: Der „Data Encryption Standard“ ist ein Datenverschlüsselungsstandard.

Datenkompression: Zur effizienteren Übertragung (z.B. per Modem) oder zum Einsparen von Speicherplatz (z.B. auf Datenträgern) werden Daten durch spezielle Pack-Programme verlustfrei komprimiert. Bekannte Dateiformate für komprimierte Dateien und Archive sind ZIP, RAR und ARJ. Auch Viren verbreiten sich oft komprimiert und bringen dann ihre eigenen Dekomprimierungsroutinen mit.

Debugger: Ein Debugger ist ein Tool für Software-Entwickler, mit dem sie Fehler im Programmablauf aufspüren können. Das Programm lässt sich an bestimmten Punkten anhalten und schrittweise ausführen. Im Debugger werden dann die jeweiligen Werte der aktiven Variablen angezeigt.

Defacement: Böswillige Umgestaltung von Webseiten durch einen Hacker.

Denial of Service: Bei einer Denial of Service-Attacke werden Rechner (meist Webserver) mit gezielten und/oder sehr vielen Anfragen bombardiert. Dadurch können sie ihre Dienste nicht mehr ausführen und brechen unter der Last zusammen.

DES: Der „Data Encryption Standard“ ist ein Datenverschlüsselungsstandard.

DHCP: Über das „Dynamic Host Configuration Protocol“ werden automatisch feste oder dynamische IP-Adressen an Clients vergeben. Außerdem werden Gateway-Einstellungen für Netzwechsel sowie DNS-Informationen verwaltet.

DHTML: Mittels „dynamischem HTML“ können Internetseiten in Verbindung mit Active Scripting und Cascading Style Sheets auch nach dem Herunterladen im Browser verändert werden. DHTML macht das Internet bunt und schön, birgt aber auch zahlreiche Gefahren.

Dialer: Dialer sind Einwahlprogramme, die eine meist kostenpflichtige Verbindung über Modem oder ISDN-Karte, zum Internet herstellt. Meist werden Dialer für die Bezahlung von sog. Mehrwertdienste im Internet verwendet und stellen eine einfache Bezahlmethode dar. Leider wurde in der Vergangenheit mit Dialern sehr viel Schindluder getrieben: - Dialer wurden ohne Wissen des Nutzers installiert - es wurden teure Auslandsnummern verwendet - die Verbindung zum Internet wurde automatisch hergestellt und nicht wieder beendet So entstanden einigen Kunden horrenden Kosten.

DirectX: Windows-Applikation zu schnelleren Grafikkarten-Ansteuerung bei Spielen oder Multimedia-Anwendungen.

Disassembler: Wenn ein Entwickler seinen Programmcode kompiliert, wird aus dem Code der Programmiersprache ein Assembler-Code erzeugt, der dann in Maschinensprache umgewandelt wird. Disassembler wandeln Maschinencode in Assembler um. Solche Werkzeuge sind nicht nur für die Fehlersuche in Programmen gedacht. Sie sind auch für die Virenanalyse sehr wichtig.

Disk And Execution MONitor: Der „Disk And Execution MONitor“ ist ein Programm, das im Hintergrund eines Netzwerks auf bestimmte Ereignisse wartet und bei Eintritt eines solchen Ereignisses bestimmte Aktionen startet. So wartet ein Mailer Daemon etwa auf eingehende E-Mails und ein Spooler wartet auf Druckaufträge.

Disk Operating System: Als „Disk Operating System“ wird generell ein Computerbetriebssystem bezeichnet, welches die Grundlage für Programme darstellt, die auf dieses Betriebssystem aufsetzen. MS-DOS, Windows Vista, OS/2, UNIX und LINUX sind z.B. „Disk Operation Systems“.

DNS: Das „Domain Name System“ ist ein Protokoll zur Umwandlung von Host-Namen in IP-Adressen. Der dazugehörige DNS-Server ordnet auf diese Weise den schwer erinnerbaren IP-Adressen (z.B.: 193.98.145.50) Host-Namen (z.B.: www.Antiviruslab.com) als Alias zu und regelt die entsprechende Verwaltung.

Domain: Domains sind die Klartextnamen für die IP-Adressen. Sie bestehen aus 3 Teilen, die durch Punkte voneinander getrennt sind: Die letzten Buchstaben bezeichnen die Top Level Domains. Sie stehen für einzelnen Länder (.de, .fr) oder Sachgruppen (.mil, .gov, .info). An vorletzter Stelle stehen die Second Level Domains mit einfach zu merkenden Begriffen (z.B. Firmennamen). Im ersten Teil des Domainnamens stehen die Namen von Rechnern und Subnetzen. Domainnamen müssen mindestens 3 und dürfen maximal 128 Zeichen lang sein und dürfen bis auf Unterstrich und Bindestrich keine Sonderzeichen oder Satzzeichen enthalten. Neuerdings sind auch deutsche Umlaute erlaubt.

Domain Name System: Das „Domain Name System“ ist ein Protokoll zur Umwandlung von Host-Namen in IP-Adressen. Der dazugehörige DNS-Server ordnet auf diese Weise den schwer erinnerbaren IP-Adressen (z.B.: 193.98.145.50) Host-Namen (z.B.: www.Antiviruslab.com) als Alias zu und regelt die entsprechende Verwaltung.

DoS: Bei einer Denial of Service-Attacke werden Rechner (meist Webserver) mit gezielten und/oder sehr vielen Anfragen bombardiert. Dadurch können sie ihre Dienste nicht mehr ausführen und brechen unter der Last zusammen.

DOS: Als „Disk Operating System“ wird generell ein Computerbetriebssystem bezeichnet, welches die Grundlage für Programme darstellt, die auf dieses Betriebssystem aufsetzen. MS-DOS, Windows Vista, OS/2, UNIX und LINUX sind z.B. „Disk Operation Systems“.

Duplex: „Duplex“ ist ein alter Begriff aus den Ursprüngen der Telekommunikation. „Duplex“ bedeutet, dass eine Kommunikation zwischen zwei Stationen gleichzeitig in beide Richtungen möglich ist. „Simplex“ bedeutet, dass eine Kommunikation jeweils nur in eine Richtung möglich ist und Halbduplex“ bezeichnet eine Datenübertragung bzw. Kommunikation in beide Richtungen, aber nicht gleichzeitig.

Dynamic Host Configuration Protocol: Über das „Dynamic Host Configuration Protocol“ werden automatisch feste oder dynamische IP-Adressen an Clients vergeben. Außerdem werden Gateway-Einstellungen für Netzwechsel sowie DNS-Informationen verwaltet.

Dynamic HTML: Mittels „dynamischem HTML“ können Internetseiten in Verbindung mit Active Scripting und Cascading Style Sheets auch nach dem Herunterladen im Browser verändert werden. DHTML macht das Internet bunt und schön, birgt aber auch zahlreiche Gefahren.

Egress Filtering: In einer Firewall kann man sowohl den vom Internet (oder anderen Netzwerken) eingehenden Traffic filtern als auch den Traffic, der das eigene Netzwerk verlässt. Unter Egress Filtering versteht man das Filtern des ausgehenden

Datenstroms. Dabei wird sichergestellt, dass alle Pakete, die das eigene Netz verlassen auch wirklich vom eigenen Netz stammen. Wäre dies gängige Praxis, wäre es leichter, DDoS-Angriffe und Netzwerk-Würmer wie SQL-Slammer und CodeRed zu stoppen.

E-Mail: „Electronic mail“ oder elektronische Post ist eine der Hauptanwendungen des Internet. Zahllose geschäftliche und private Briefe werden täglich auf elektronischem Weg verschickt. E-Mails sind aber nicht nur nützlich, sondern auch ein Hauptweg zur Verbreitung von schädlichen Programmen. Würmer verbreiten sich häufig dadurch, dass sie automatisch E-Mails versenden, deren Anhang den Wurm enthält oder auf eine Webseite mit schädlichen Inhalten verweist. Die Virenautoren versuchen dabei den Leser der E-Mail mit allen Mitteln der Tarnung und Täuschung dazu zu bringen, die Datei im Anhang zu öffnen. Es gibt aber auch E-Mails, die Sie dazu verleiten, Webseiten mit infizierten Inhalten zu besuchen. Es gibt sogar HTML-E-Mails, die den Wurm beim Öffnen der E-Mail installieren. Um dieser Gefahr zu begegnen, beinhaltet G DATA AntiVirus Schutzmechanismen für E-Mail-Programme, die den Virus schon erkennen und beseitigen, bevor er vom Nutzer unbeabsichtigt gestartet werden kann.

Ethernet: Mit der „Ethernet“-Hardware können Computer unterschiedlichster Bauart miteinander vernetzt werden.

Exploit: Ein Programm, das eine bestehende Sicherheitslücke im Zielrechner ausnutzt, um beliebigen Programmcode auszuführen.

FAQ: Ein FAQ beantwortet häufig gestellte Fragen (engl. frequently asked questions) zu einem bestimmten Thema.

FAT: Die Dateizuordnungstabelle (File Allocation Table) besteht aus aufeinanderfolgenden Sektoren eines logischen Laufwerks und enthält eine Tabelle der Zuordnung von Dateien zu logischen Sektoren des Datenträgers. Sie befindet sich in den Sektoren nach dem Bootsektor. Zusätzlich enthält sie Informationen über freie und defekte Sektoren des Datenträgers.

File Transfer Protocol: Das „File Transfer Protocol“ (= Protokoll zur Dateiübertragung) ist ein Übertragungsprotokoll für den Datenaustausch zwischen zwei Computern. FTP ist unabhängig vom Betriebssystem und der Art der Übertragung. Anders als beispielsweise HTTP, baut FTP eine Verbindung auf und hält diese während der kompletten Übertragung aufrecht.

Firewall: Bei Firewalls handelt es sich in der Regel um Software-Produkte, die den Datenstrom zwischen einem Rechner im lokalen Intranet (z.B. ein Firmennetzwerk oder ein einzelner Heimcomputer) und Rechnern in offeneren Netzen (z.B. dem Internet) reglementieren und dafür sorgen, dass ungewünschte Inhalte (z.B. auch Dateien, die potentiell Viren enthalten können) nicht übertragen werden können. Oft wird dazu der Traffic auf vielen Ports unterbunden.

Flame: E-Mails mit beleidigendem Inhalt werden als Flames bezeichnet.

Flooding: Flooding gilt als Oberbegriff für verschiedene Möglichkeiten, bestimmte Rechner innerhalb eines Netzes durch Überforderung zu behindern bzw. zu überlasten.

FTP: Das „File Transfer Protocol“ (= Protokoll zur Dateiübertragung) ist ein Übertragungsprotokoll für den Datenaustausch zwischen zwei Computern. FTP ist unabhängig vom Betriebssystem und der Art der Übertragung. Anders als beispielsweise HTTP, baut FTP eine Verbindung auf und hält diese während der kompletten Übertragung aufrecht.

FTP-Server: Auf „FTP-Servern“ werden Internetanwendern Dateien und Verzeichnisse zum Download bereitgestellt. Auf öffentlichen FTP-Servern kann man sich oftmals mit der Benutzerkennung „Anonymous“ und der eigenen E-Mail-Adresse als Passwort anmelden. Einige Viren und Trojaner installieren eigene FTP-Server, mit denen sie Dateien vom infizierten PC herunterladen können.

Gateway: Ein „Gateway“ stellt eine Schnittstelle zwischen verschiedenen Kommunikationssystemen dar, z.B. einem Intranet mit dem Internet.

Gopher: Gopher ist der Name eines speziellen Informationsdienst, der im Internet angeboten wurde bevor sich das HTTP Protokoll durchgesetzt hat; Wörtlich übersetzt heißt Gopher „Erdhörnchen“. Eine Interpretation als „go“ und „for“ im Sinne von „etwas holen“ trifft die Funktion des Protokolls genauer. Inzwischen wird Gopher allerdings durch intelligentere Suchsysteme im WWW weitgehend verdrängt.

HBCI: Das „Home Banking Communication Interface“ ist ein Internet-Protokoll zur gefahrlosen Kommunikation von Bank und Bankkunde untereinander.

Header: Der „Header“ bezeichnet den Kopfteil einer Datei und beinhaltet Informationen zur Datei. In E-Mails stehen im Header u.a. Absender, Empfänger und Betreff.

Heuristik: In der heuristischen Analyse werden Viren nicht nur anhand der ständig aktualisierten Virendatenbanken ermittelt, sondern auch anhand bestimmter virentypischer Merkmale. Diese Methode ist ein weiteres Sicherheitsplus, kann in seltenen Fällen aber auch zu mehr Fehlalarmen führen.

Hijacker: Hijacker installieren sich unbemerkt und ändern Einstellungen des Browsers (z.B. die Startseite) und dessen Funktionen (z.B. Suchfunktion). Daher gehören sie eigentlich zu den Trojanern. Browser Hijacker leiten den Nutzer ungewollt auf (oft pornografische) Webseiten indem die Startseite oder die Suchfunktion umgeleitet wird. Manchmal werden auch zusätzliche Menüleisten oder Fenster angezeigt, die sich nicht entfernen oder schließen lassen. Oft nutzen Browser Hijacker Sicherheitslücken und Schwachstellen des Systems, um sich tief darin einzunisten. Meist wird der Internet Explorer angegriffen. Die Beseitigung der Fehlfunktionen ist oft sehr umständlich. Einer der berühmtesten Browser Hijacker ist CoolWeb.

Hoax: Hoaxes sind angebliche Warnungen vor Viren und anderen Gefahren, die oftmals per E-Mail verbreitet werden. Die Empfänger werden aufgefordert die E-Mail-Warnung an Freunde und Bekannte weiterzuleiten. Meistens handelt es sich bei diesen Mitteilungen um Panikmache, die nur Zeit (und damit Geld) kosten.

Home Banking Communication Interface: Das „Home Banking Communication Interface“ ist ein Internet-Protokoll zur gefahrlosen Kommunikation von Bank und Bankkunde untereinander.

Hop: Als Hop bezeichnet man einen Rechner oder Knotenpunkt über den ein Datenpaket läuft, das von einem Rechner zu einem anderen geschickt wird.

Host: Host bezeichnet den Rechner, der dem Anwender die Möglichkeit bietet, Dienste (z.B. E-Mail) in Anspruch zu nehmen bzw. eine Datenverbindung (z.B. ins Internet) zu eröffnen.

HTML: Die HyperText Markup Language ist eine Seitenbeschreibungssprache des WWW und ermöglicht das Aussehen und Verhalten von Dokumenten plattformübergreifend zu regeln. HTML-Dateien werden innerhalb des WWW über HTTP übertragen.

HTTP: Das Hyper Text Transfer Protocol ist ein Client/Server-Protokoll, das im WWW zum Austausch von HTML-Dokumenten dient.

HTTPS: Das Hyper Text Transfer Protocol (Secure) dient, wie HTTP zum Austausch von HTML-Dokumenten, verschlüsselt die Daten aber vor der Übertragung.

Hub: Ein Hub ist ein Gerät um Computer oder Peripheriegeräte sternförmig miteinander zu vernetzen.

Hyperlink: Während ein Link innerhalb eines HTML-Dokuments auf einen anderen Textabschnitt verweist, stellt der Hyperlink die Möglichkeit dar, vom aktuellen Dokument in ein anderes Dokument innerhalb des WWW zu wechseln.

Hypertext: Hypertext ist die Bezeichnung für ein Dokument, in welchem durch Querverweise (Links) ein nichtlineares Lesen ermöglicht wird.

HyperText Markup Language: Die HyperText Markup Language ist eine Seitenbeschreibungssprache des WWW und ermöglicht das Aussehen und Verhalten von Dokumenten plattformübergreifend zu regeln. HTML-Dateien werden innerhalb des WWW über HTTP übertragen.

HyperText Transfer Protocol: Das Hyper Text Transfer Protocol ist ein Client/Server-Protokoll, das im WWW zum Austausch von HTML-Dokumenten dient.

HyperText Transfer Protocol Secure: Das Hyper Text Transfer Protocol (Secure) dient, wie HTTP zum Austausch von HTML-Dokumenten, verschlüsselt die Daten aber vor der Übertragung.

IANA: Die „Internet Assigned Numbers Authority“ ordnet bestimmten Ports des TCP/IP-Protokolls bestimmte Dienste zu. Beispielsweise wird aus dieser Übereinkunft heraus für das HTTP-Protokoll Port 80 verwendet und für FTP Port 20/21.

ICMP: Das Internet Control Message Protocol ermöglicht das Versenden von Fehlermeldungen sowie Test- und Informationspaketen und ist ein Teil des TCP/IP.

ICP: Das „Internet Cache Protocol“ regelt die Kommunikation von Cacheservern und Proxyservern mit den Clients.

IE: Der Internet Explorer ist ein Web-Browser von Microsoft.

IMAP: Das Internet Message Access Protokoll (IMAP) ist eine Weiterentwicklung des POP-Protokolls und ermöglicht es, Nachrichten bedarfsweise zu übermitteln. Dazu werden erst die Kopfzeilen von Mails übermittelt und erst dann wird entschieden, wie mit der eigentlichen Mail zu verfahren ist.

In the wild: Viren die sich ‚in the wild‘ befinden, sind solche, die bei PC-Nutzern tatsächlich auftreten. Im Unterschied zu Zoo-Viren, die nur in Sammlungen von Virenautoren und Herstellern von Antiviren-Software existieren, aber nie verbreitet wurden. Derzeit verbreitete Viren werden in die „Wildlist“ von www.wildlist.org aufgenommen.

Internet: Das Internet ist ein weltweiter Verbund von Millionen Rechnern und hat sich vom militärisch genutzten Arpanet zu einem lebensbestimmenden kultur- und ländergrenzenüberspannenden Netzwerk entwickelt.

Internet Assigned Numbers Authority: Die „Internet Assigned Numbers Authority“ ordnet bestimmten Ports des TCP/IP-Protokolls bestimmte Dienste zu. Beispielsweise wird aus dieser Übereinkunft heraus für das HTTP-Protokoll Port 80 verwendet und für FTP Port 20/21.

Internet Cache Protocol: Das „Internet Cache Protocol“ regelt die Kommunikation von Cacheservern und Proxyservern mit den Clients.

Internet Control Message Protocol: Das Internet Control Message Protocol ermöglicht das Versenden von Fehlermeldungen sowie Test- und Informationspaketen und ist ein Teil des TCP/IP.

Internet Explorer: Der Internet Explorer ist ein Web-Browser von Microsoft.

Internet Message Access Protokoll: Das Internet Message Access Protokoll (IMAP) ist eine Weiterentwicklung des POP-Protokolls und ermöglicht es, Nachrichten bedarfsweise zu übermitteln. Dazu werden erst die Kopfzeilen von Mails übermittelt und erst dann wird entschieden, wie mit der eigentlichen Mail zu verfahren ist.

Internet Relay Chat: Über das Internet Relay Chat-Protokoll können zwei oder mehrere Personen über das Internet eine Textkommunikation in Echtzeit durchführen.

IP-Adresse: Die Internet Protocol-Adresse ist eine numerische Adresse zur Identifizierung von Rechnern in einem TCP/IP-Netz. Diese Adresse wird in vier Byte dargestellt (z.B. 193.98.145.50). Sie besteht dabei aus zwei Teilen: 1. Adresse des logischen Netzwerks 2. Adresse eines Hosts innerhalb des logischen Netzwerks. Da Menschen sich IP-Adressen nicht so gut merken können, verwenden sie normalerweise Domainnamen um im Rechner im Internet zu besuchen.

IPX/SPX: Internet Packet Switching Protocol / Service Packet Switching Protocol
IPX/SPX bezeichnet ein Netzwerkprotokoll, das von Novell entwickelt wurde.

IRC: Über das Internet Relay Chat-Protokoll können zwei oder mehrere Personen über das Internet eine Textkommunikation in Echtzeit durchführen.

ISDN: Als „Integrated Services Digital Network“ wird ein internationaler Standard für digitale Fernsprechnetze bezeichnet, über den Telefongespräche, Datenfernübertragung und andere Mehrwertdienste abgewickelt werden können. ISDN stellt eine Weiterentwicklung des analogen Telefonnetzes dar und bietet jedem Anwender zwei Basiskanäle mit jeweils 64 kBit Übertragungskapazität und einen Steuerkanal mit 16 kBit.

ISP: Die Internet Service Provider sind Anbieter und Verwalter von Internet Zugängen.

ITW: Viren die sich ‚in the wild‘ befinden, sind solche, die bei PC-Nutzern tatsächlich auftreten. Im Unterschied zu Zoo-Viren, die nur in Sammlungen von Virenautoren und Herstellern von Antiviren-Software existieren, aber nie verbreitet wurden. Derzeit verbreitete Viren werden in die „Wildlist“ von www.wildlist.org aufgenommen.

Java: Java ist eine objektorientierte Programmiersprache, die es aufgrund Ihrer Plattform-Unabhängigkeit ermöglicht, Anwendungen zu erstellen, die auf den unterschiedlichsten Computersystemen funktionsfähig sind.

JavaScript: Eine mit Java nur entfernt verwandte Skriptsprache. Sie bietet eine Möglichkeit HTML um Active Scripting zu erweitern. Webseiten können im Browser (also clientseitig) nach dem Laden der Seite dynamisch verändert werden. Leider eröffnet JavaScript Sicherheitslücken wie z.B. Zugang zu Systeminformationen oder Ausführung von Programmen.

JavaScript Style Sheet: JavaScript StyleSheet bezeichnet eine von Netscape vorgeschlagene JavaScript- Modifikation. Um eine Kompatibilität des JavaScripts mit CSS zu erreichen.

JPEG: Das Grafikformat der „Joint Photographics Experts Group“ ist im Internet weit verbreitet, da es aufgrund ausgefeilter Kompressionsalgorithmen die Möglichkeit beinhaltet, große Bilder bei vollem Farbumfang als relativ kleine Dateien zu speichern.

JPG: Das Grafikformat der „Joint Photographics Experts Group“ ist im Internet weit verbreitet, da es aufgrund ausgefeilter Kompressionsalgorithmen die Möglichkeit beinhaltet, große Bilder bei vollem Farbumfang als relativ kleine Dateien zu speichern.

JScript: Jscript stellt eine für die Belange des Internet Explorer modifizierte Version von JavaScript dar.

JSSS: JavaScript StyleSheet bezeichnet eine von Netscape vorgeschlagene JavaScript- Modifikation. Um eine Kompatibilität des JavaScripts mit CSS zu erreichen.

Kaltstart: Starten des PCs nachdem der Rechner ausgeschaltet (und daher meistens abgekühlt) war. Der Inhalt des Arbeitsspeicher wird dabei im Gegensatz zum Warmstart vollständig gelöscht und damit auch speicherresidente Viren.

KBit: Ein KiloBit sind 1024 Bit.

KByte: Ein KiloByte sind 1024 Byte.

Kermit: Kermit benannt nach „Kermit“ dem Frosch aus der ‚Muppet Show‘, ist das älteste Übertragungsprotokoll überhaupt. Es findet auch heute noch Verwendung, weil viele alte Großrechner nur mit Kermit ansprechbar sind.

Keylogger: Mit einem Keylogger werden Tastatureingaben aufgezeichnet und ggf. versendet. So lassen sich Passwörter und andere persönliche Daten erschnüffeln. Ein Vertreter dieser Spezies heißt Padodoor.

Kompression: Durch Komprimierung (also zusammenpressen) kann das Datenvolumen einer Datei teilweise erheblich verringert werden. Das spart Platz beim Archivieren und Bandbreite beim Übertragen von Dateien. Nachteil dieser Platzersparnis ist, dass auf diese Datei dann nur noch mit entsprechender Dekompressionssoftware wie z.B. WinZip, WinRAR oder ARJ zugegriffen werden kann.

Komprimierung: Durch Komprimierung (also zusammenpressen) kann das Datenvolumen einer Datei teilweise erheblich verringert werden. Das spart Platz beim Archivieren und Bandbreite beim Übertragen von Dateien. Nachteil dieser Platzersparnis ist, dass auf diese Datei dann nur noch mit entsprechender Dekompressionssoftware wie z.B. WinZip, WinRAR oder ARJ zugegriffen werden kann.

Kontextmenü: Das Kontextmenü erhalten Sie, wenn Sie mit der rechten Maustaste in bestimmte Bereiche einer Programmoberfläche klicken. Im Kontextmenü können Sie dann Aktionen auswählen, die mit dem angeklickten Objekt durchgeführt werden können.

Konvertierung: Die Umwandlung eines Dateityps in eine Datei mit gleichem Inhalt aber anderem Format wird als Konvertierung bezeichnet.

LAN: Das „Local Area Network“ ist ein Netzwerk, das auf ein überschaubares Areal begrenzt ist; z.B. ein Firmengebäude oder -gelände.

LASE: Eine Limited Area Search Engine bezeichnet einen Web-Katalog der sich auf ein explizites Gebiet spezialisiert und darum in der Regel durch ein auf diesem Gebiet kompetentes und fachlich versiertes Team zusammengestellt ist.

Laufzeitfehler: Ein ‚run time error‘ (engl. Laufzeitfehler) ist ein Fehler, der auftritt, während ein Programm ausgeführt wird. Meist muss die Applikation nach einem Laufzeitfehler beendet werden. Im schlimmsten Fall muss der Rechner neu gebootet werden. Andere Fehler treten auf, wenn das Programm kompiliert (compile time error) wird.

Limited Area Search Engine: Eine Limited Area Search Engine bezeichnet einen Web-Katalog der sich auf ein explizites Gebiet spezialisiert und darum in der Regel durch ein auf diesem Gebiet kompetentes und fachlich versiertes Team zusammengestellt ist.

Lineare Verbindung: Lineare Verbindungen bezeichnen den Zusammenschluss mehrerer Festplatten zu einer großen Partition. Auf diese Art und Weise ist es möglich, sehr große Partitionen zu bilden.

Link: Ein Link bezeichnet die Verknüpfung zwischen zwei HTML-Dokumenten. Er ist ein Spezialfall eines URL (Uniform Resource Locator).

LiveScript: Als „LiveScript“ wurde das aktuelle JavaScript während seiner Entwicklungsphase bei Netscape bezeichnet.

Local Area Network: Das „Local Area Network“ ist ein Netzwerk, das auf ein überschaubares Areal begrenzt ist; z.B. ein Firmengebäude oder -gelände.

Login: Der Vorgang der Einwahl, Anmeldung und Authentifizierung (meist per Passwort) eines Anwenders an ein Computersystem wird „LogIn“ genannt.

Logoff: Das Beenden einer Datenverbindung zu einem Computersystem bezeichnet man als „LogOff“.

Mac OS: Betriebssystem von Apple Macintosh Computern.

MAC-Adresse: Die MAC-Adresse (Media Access Control) ist die Hardware-Adresse eines Netzwerkgerätes (z.B. Netzwerkkarte, Switch). Die Mac-Adresse ist weltweit eindeutig. Sie besteht aus 48 bit in denen der Hersteller des Gerätes (24 Bit) und vom Hersteller verwendete Schnittstellen identifiziert werden. So lässt sich das Gerät eindeutig im Netzwerk identifizieren. Oft wird die MAC Adresse zur Erzeugung von Lizenzschlüsseln für Software verwendet.

Mailbomb: Der schädliche Code wird einem ahnungslosen Nutzer per Mail zugesandt.

Mailbox: Eine Mailbox ist ein Computersystem, das E-Mail-Dienste, Chat und Dateidownloads über eine bestimmte Einwahlnummer anbietet und nicht mit dem Internet verbunden ist.

Mailingliste: Mailinglisten stellen einen ggf. moderierten Verbund verschiedener E-Mail-Empfänger dar. Eine E-Mail an die Mailingliste erreicht dabei stets alle Abonnenten der Mailinglist. Die meisten Mailinglisten beschäftigen sich mit einem eng umgrenzten Thema.

MAPI: Die „Messaging API“ regelt die Kommunikation zwischen Windows-Anwendungen und Microsoft Mail.

MB: Ein MegaByte sind 1024 KByte.

MBit: Ein MegaBit sind 1024 KBit.

MByte: Ein MegaByte sind 1024 KByte.

Media Access Control: Die MAC-Adresse (Media Access Control) ist die Hardware-Adresse eines Netzwerkgerätes (z.B. Netzwerkkarte, Switch). Die Mac-Adresse ist weltweit eindeutig. Sie besteht aus 48 bit in denen der Hersteller des Gerätes (24 Bit) und vom Hersteller verwendete Schnittstellen identifiziert werden. So lässt sich das Gerät eindeutig im Netzwerk identifizieren. Oft wird die MAC Adresse zur Erzeugung von Lizenzschlüsseln für Software verwendet.

MegaByte: Ein MegaByte sind 1024 KByte.

Message: Message bedeutet übersetzt „Nachricht, Botschaft“, und bezeichnet in der Regel eine E-Mail Nachricht oder eine Instant Message.

MIME: „Multipurpose Internet Mail Extensions“ ist eine Kodierung zur Kombination von E-Mails mit Binärdateien. Sobald Absender und Adressat ein MIME-fähiges E-Mail-Programm verwenden, können Sie Binärdateien wie z.B. ausführbare EXE Dateien, gezippte Archive oder DOC Dateien von Word direkt in E-Mails einfügen.

MMX: „MultiMedia eXtensions“-Prozessoren sind extra für Multimedia-Anwendungen (Spiele, Grafik, Video) optimiert und bieten hierbei einen beschleunigten Programmablauf.

Modem: Mit Hilfe eines „MOdulator / DEModulators“ lassen sich Computer für die Datenfernübertragung aufrüsten. Die Modem-Hardware ermöglicht - mit entsprechender Software - die Einwahl ins Internet oder andere lokale oder offene Computernetzwerke.

MPEG: Ein von der „Motion Picture Experts Group“ entwickelter Kompressionsstandard für die digitale Verarbeitung von Audio- und Videodaten.

MultiMedia eXtensions: „MultiMedia eXtensions“-Prozessoren sind extra für Multimedia-Anwendungen (Spiele, Grafik, Video) optimiert und bieten hierbei einen beschleunigten Programmablauf.

Multipurpose Internet Mail Extensions: „Multipurpose Internet Mail Extensions“ ist eine Kodierung zur Kombination von E-Mails mit Binärdateien. Sobald Absender und Adressat ein MIME-fähiges E-Mail-Programm verwenden, können Sie Binärdateien wie z.B. ausführbare EXE Dateien, gezippte Archive oder DOC Dateien von Word direkt in E-Mails einfügen.

NAT: Die Network Address Translation ermöglicht es, private IP-Adressen eines Local Area Networks auf öffentliche IP-Adressen umzusetzen. Auf diese Weise ist es z.B. möglich, mehrere Rechner über eine einzige, vom Provider gelieferte IP-Adresse ins Internet zu bringen.

Netiquette: „Netiquette“ ist eine Wortschöpfung, die sich aus „Netz“ und „Etiquette“ ableitet und eine Art Verhaltenskodex im Internet bezeichnet. Im Prinzip gelten laut der Netiquette dieselben grundlegenden Höflichkeitsformen wie im echten Leben (RL = real life), bloß dass diese aufgrund der einfachen Möglichkeiten zur Anonymisierung der Teilnehmer offenbar einer besonderen Erwähnung bedürfen.

Network Address Translation: Die Network Address Translation ermöglicht es, private IP-Adressen eines Local Area Networks auf öffentliche IP-Adressen umzusetzen. Auf diese Weise ist es z.B. möglich, mehrere Rechner über eine einzige, vom Provider gelieferte IP-Adresse ins Internet zu bringen.

Netzwerk: Als „Netzwerk“ wird ein Verbund von Computern und Peripheriegeräten bezeichnet, die auf Basis eines gemeinsamen Netzprotokolls miteinander kommunizieren können.

Newsgroup: Newsgroups sind Öffentliche Diskussionsforen im Internet zu eng umrissenen Themen. Sie sind die Nachfolger des Usenet.

NIC: Die „Network Information Center“ sind für die Vergabe von IP-Adressen verantwortlich. Für Deutschland erfolgt dies durch die DE-NIC. Für allgemeine Toplevel Domains ist die Inter-NIC verantwortlich.

NNTP: Das Network News Transfer Protocol entwickelt sich gegenwärtig zum Standard im Internet. Damit verdrängt NNTP das alte News-Protocol.

NullSession: Von NullSessions spricht man, wenn bei der Anmeldung an einem fremden System kein Nutzernamen und kein Passwort angegeben wird. Windows NT/2000/XP/Server2003 stellt dann dem anfragenden System etliche Informationen

zur Verfügung. U.a. Domainname, Adresse(n) des Rechners uvm. Diese NullSessions sind Grundlage für einige Windows-Funktionen. Sie bieten allerdings auch eine Reihe konzeptueller Schwachstellen, die von einem Cracker ausgenutzt werden können, um unbefugt auf die Daten eines Rechners zuzugreifen. Mehr dazu in einem Artikel von Joe Finamore.

OCX: ActiveX bezeichnet eine Technologie, die auf dem Component Object Model (COM) von Microsoft beruht. Sie ermöglicht es Softwarekomponenten, miteinander zu interagieren, auch wenn sie von unterschiedlichen Personen, zu unterschiedlichen Zeiten, mit unterschiedlichen Tools in unterschiedlichen Programmiersprachen geschrieben wurden. Die Komponenten - auch ActiveX Steuerelemente (engl. ActiveX Controls) genannt - müssen noch nicht einmal auf dem gleichen Rechner vorhanden sein. Durch ihren modularen Charakter lassen sich ActiveX Controls einfach in eigene Programme einbinden. Der Programmierer muss dazu lediglich die Spezifikation der Schnittstelle kennen. Nicht nur in Anwendungen von Microsoft werden ActiveX Controls eingesetzt. Sie werden z.B. dafür verwendet, um Word-, Excel- oder PowerPoint-Dokumente im Internet Explorer zu öffnen. Man spricht dann von ActiveX Dokumenten.

ODBC: Open Database Connectivity sind Schnittstellen die von Microsoft entwickelt wurden. Mit Hilfe dieser Schnittstellen kann auf SQL-Datenbanken zugegriffen werden.

Offline: Offline bedeutet, dass ein Client-Rechner keine Verbindung zum Server oder dem Internet hat.

Offline-Reader: Über „Offline-Reader“ kann man Informationen aus dem Internet auf den lokalen Rechner herunterladen. Nach dem Download kann man auch ohne Internetverbindung die ausgewählten Webseiten in Ruhe lesen oder durchstöbern. Dies hat den Vorteil, dass während dieser Zeit keine Verbindungs- und Providerkosten anfallen.

Online: Ein Rechner ist online wenn er eine Verbindung (z.B. über Telefonleitung) zum Server oder dem Internet hat.

OSI Schichtenmodell: Das OSI-Modell (engl. Open Systems Interconnection Reference Model) ist ein Modell zur Datenübertragung zwischen verschiedenen Computersystemen. Es besteht aus 7 unabhängigen Schichten, die jeweils für bestimmte Aufgaben zuständig sind. Die höheren Schichten beruhen auf den niedrigeren: 1. Physikalische Schicht, 2. Sicherungsschicht, 3. Netzwerkschicht, 4. Transportschicht, 5. Sitzungsschicht, 6. Darstellungsschicht, 7. Anwendungsschicht.

P2P: Bei „Peer to Peer“-Netzwerken existiert kein zentraler Server und alle Computer im Verbund agieren gleichberechtigt nebeneinander.

Packet INternet Grouper: Mit dem Packet Internet Grouper können IP-Verbindungen getestet werden. Der Befehl ping gibt die Dauer an, wie lange ein Packet unterwegs ist. Für Online-Spieler interessant: Je kleiner der Ping-Wert, desto schneller (=besser) ist die Verbindung.

Packeting: Eine Form des Flooding, bei der ICMP-Pakete an bestimmte IP-Adressen gesendet werden, um auf diese Weise einen Denial of Service zu erreichen.

Pageview: Als Pageview bezeichnet man die Übersicht von Besuchen auf einer Seite. Alle Besuche einer Seite werden zur Pageview (der jeweiligen Seite) summiert, die dadurch zur Ermittlung von Besucherzahlen auf einer Website benutzt werden kann. Den Gegensatz zum Pageview stellen die Hits dar, die nicht alle Anfragen auf einer Seite, sondern alle Anfragen einer IP (also eines Users) zählen.

PAP: Das Password Authentication Protocol dient als Teil der IETF-Protokollsuite, dem Austausch von Passwörtern. Weil das PAP das User-Passwort unkodiert zur Überprüfung an einen zentralen Server überträgt, bietet es nur einen geringen Schutz.

PAP: Das Printer Access Protocol ist ein Bestandteil der AppleTalk Protokoll-Suite. Es überträgt Druckdaten und fragt Konfigurations- und Zustandsinformationen vom netzwerkfähigen Drucker ab.

Password Authentication Protocol: Das Password Authentication Protocol dient als Teil der IETF-Protokollsuite, dem Austausch von Passwörtern. Weil das PAP das User-Passwort unkodiert zur Überprüfung an einen zentralen Server überträgt, bietet es nur einen geringen Schutz.

Patch: Ein Patch behebt Fehler oder schließt Sicherheitslücken in einer Software. Das Patch ersetzt dabei nur die fehlerhaften Dateien und ersetzt nicht die Vollversion der Software.

Payload: Payload ist die englische Bezeichnung für die Schadensfunktion eines Virus (iWS). Die Auslösung der Schadensfunktion kann mit einer Bedingung, dem sog. Payload-Trigger verbunden sein. Die Definition von Schadensfunktion ist umstritten, da einige Forscher auch den Verbrauch von Systemressourcen und Übertragungsbandbreite als Payload ansehen.

Payload-Trigger: Bedingung, die einen Payload auslöst. Oft ist es ein Datum oder die Anzahl von Programmaufrufen.

PDC: Der Primary Domain Controller verwaltet als Server innerhalb eines Windows-Netzwerkes, die Benutzer und deren Rechte.

PDF: Das „Portable Document Format“ ist ein von Adobe entwickeltes Format, um bebilderte Texte auf verschiedenen Rechnersystemen gleichartig darstellen zu können.

PE Datei: Portable Executable. Ausführbare Datei für Win32 Betriebssysteme. Nachfolger der ausführbaren Dateien unter DOS (.EXE und .COM).

Peer: Bei einem Netzwerk ohne zentralen Server bezeichnet man die jeweils andere Station einer Vernetzung als „Peer“.

Peer-to-Peer: Bei „Peer to Peer“-Netzwerken existiert kein zentraler Server und alle Computer im Verbund agieren gleichberechtigt nebeneinander.

Perl: Perl (Practical Extraction and Report Language) ist eine Programmiersprache, die ursprünglich zur Auswertung von Logdateien entwickelt wurde und ihre Stärken in der Textverarbeitung mit regulären Ausdrücken hat. Mittlerweile hat Perl sich zu einer leistungsstarken Programmiersprache entwickelt. Perl wird häufig zur CGI-Programmierung im Internet eingesetzt.

Personal Identification Number: Die „Personal Identification Number“ dient z.B. beim Online-Banking oder bei Mobiltelefonen zur Identifikation des Nutzers.

PGP: Als „Pretty Good Privacy“ wird ein Programm zur Verschlüsselung von Daten bezeichnet, das auf dem Public - Private Key Prinzip basiert. Dabei können Nachrichten mit dem Public Key (öffentlichen Schlüssel) verschlüsselt, anschließend allerdings nur mit dem Private Key (privaten Schlüssel) entschlüsselt und gelesen werden.

Phishing: Unter Phishing versteht man den Versuch persönliche Daten wie Loginnamen, Passwörter, Kreditkartennummern, Bankzugangsdaten etc. durch gefälschte Webseiten oder unerwünschte E-Mails zu erhalten. Meist richten sich Phishing-Versuche an Kunden von Banken mit Online-Banking Angeboten (CityBank, Postbank), Bezahlendienste (Paypal), Internet Service Provider (AOL) oder Online-Shops (eBay, Amazon). Oft wird man dazu per E-Mail oder Instant Messenger auf gefälschte Webseiten geleitet, die den Seiten der Vorbilder sehr genau nachempfunden sind.

PIN: Die „Personal Identification Number“ dient z.B. beim Online-Banking oder bei Mobiltelefonen zur Identifikation des Nutzers.

Ping: Mit dem Packet Internet Grouper können IP-Verbindungen getestet werden. Der Befehl ping gibt die Dauer an, wie lange ein Packet unterwegs ist. Für Online-Spieler interessant: Je kleiner der Ping-Wert, desto schneller (=besser) ist die Verbindung.

Point to Point Protocol: Das „Point to Point Protocol“ ist ein Übertragungsprotokoll, das die Verbindung zwischen dem Modem eines Computeranwenders und dem Einwahlknoten eines Providers regelt.

Polymorphe Viren: Polymorphe Viren enthalten Mechanismen, um ihr Aussehen bei jeder Infektion zu verändern. Dazu gehört unter anderem der Austausch von Befehlssequenzen und zufallsgesteuertes Einstreuen von unsinnigen Befehlsgruppen. Diese sind in keiner Weise für das Funktionieren des Virus erforderlich. So können leicht Milliarden von Varianten eines Virus entstehen. Um verschlüsselte und polymorphe Viren sicher zu erkennen und zu beseitigen, reicht der Einsatz klassischer Virensignaturen häufig nicht aus. Meist müssen spezielle Programme geschrieben werden. Der Aufwand zur Analyse und zur Bereitstellung geeigneter Gegenmittel kann dabei extrem hoch sein. So sind polymorphe Viren ohne Übertreibung als die Königsklasse unter den Viren zu bezeichnen.

POP3: POP3 ist die Abkürzung für „Post-Office Protocol 3“. Mit Hilfe dieses Protokolls werden E-Mail-Daten von einem E-Mail-Server mit Hilfe eines POP3-basierten E-Mail-Programms auf den Rechner des Adressaten heruntergeladen.

Pop-Up: Pop-Ups sind Browserfenster, die sich parallel zur aufgerufenen Seite öffnen. Da sie meist Werbung enthalten, kann man das Öffnen der Fenster mit sog. Pop-Up Blockern unterbinden.

Port: Vernetzte Anwendungen kommunizieren untereinander durch eine Kombination aus IP-Adresse und Port-Nummer und spezifizieren damit den Dienst,

der auf dem jeweiligen Zielrechner angesprochen werden soll. So dient z.B. in der Regel Port 80 für HTTP oder die Ports 20 und 21 für FTP. Mit einer Firewall kann der Datenaustausch für einzelne Port geregelt werden.

Portable Document Format: Das „Portable Document Format“ ist ein von Adobe entwickeltes Format, um bebilderte Texte auf verschiedenen Rechnersystemen gleichartig darstellen zu können.

Posting: Posting bezeichnet eine Nachricht, die im Internet meist in Newsgroups, Mailinglisten oder in Foren veröffentlicht wird.

Post-Office Protocol 3: POP3 ist die Abkürzung für „Post-Office Protocol 3“. Mit Hilfe dieses Protokolls werden E-Mail-Daten von einem E-Mail-Server mit Hilfe eines POP3-basierten E-Mail-Programms auf den Rechner des Adressaten heruntergeladen.

PostScript: PostScript ist eine Seitenbeschreibungssprache zur gleichartigen Ausgabe von Daten auf verschiedenen Systemen (z.B. Druckern). PostScript Dateien enden auf .PS. Um sie im Rechner anzusehen, braucht man einen PostScript Viewer wie z.B. GhostView.

PPP: Das „Point to Point Protocol“ ist ein Übertragungsprotokoll, das die Verbindung zwischen dem Modem eines Computeranwenders und dem Einwahlknoten eines Providers regelt.

Pretty Good Privacy: Als „Pretty Good Privacy“ wird ein Programm zur Verschlüsselung von Daten bezeichnet, das auf dem Public - Private Key Prinzip basiert. Dabei können Nachrichten mit dem Public Key (öffentlichen Schlüssel) verschlüsselt, anschließend allerdings nur mit dem Private Key (privaten Schlüssel) entschlüsselt und gelesen werden.

Primary Domain Controller: Der Primary Domain Controller verwaltet als Server innerhalb eines Windows-Netzwerkes, die Benutzer und deren Rechte.

Printer Access Protocol: Das Printer Access Protocol ist ein Bestandteil der AppleTalk Protokoll-Suite. Es überträgt Druckdaten und fragt Konfigurations- und Zustandsinformationen vom netzwerkfähigen Drucker ab.

Private Key: Der Private Key ist notwendig, um bei PGP mit dem Public Key verschlüsselte Dokumente, entschlüsseln zu können.

Protokoll: Ein Protokoll dient der Kommunikation zwischen verschiedenen Rechnern in einem Netzwerk. Das Protokoll enthält eine formale Zusammenstellung von Regeln, die den Nachrichtenaustausch steuern. Beispiele für Protokolle sind FTP, HTTP, POP3 oder TCP/IP.

Provider: Anbieter eines Internetzugangs.

Proxy: Der Proxy-Server stellt eine Art Zwischenspeicher dar, der dazu dient, die Menge der übertragenen Daten in einem Netzwerk zu verringern. So werden Dateien, die von vielen Anwendern heruntergeladen werden, in einem Zwischenspeicher gelagert und können auf diese Weise schneller verwendet werden, ohne dass der eigentliche Ladevorgang (z.B. aus dem Internet) erneut erfolgen

müsste. Dieser Zwischenspeicher kann in Verbindung mit einer Firewall auch für eine erhöhte Datensicherheit und einen grundlegenden Schutz vor möglicherweise virenverseuchten Dateien dienen.

Public Key: Der Public Key wird bei PGP verwendet, um Dokumente zu verschlüsseln.

Pufferüberlauf: Bei einem Buffer Overflow überflutet ein Angreifer Datenfelder mit einer zu großen Datenmenge. Unter Umständen ist es so möglich, im Speicher der Rechners eigenen Programmcode auszuführen und versteckte Befehle zu übermitteln, die dem Angreifer einen Zugang auf diesen Rechner ermöglichen.

Pulswählverfahren: Beim veralteten Pulswählverfahren wird die Rufnummer über eine Anzahl von Impulsen an die Telefonvermittlung weitergeleitet. Es ist inzwischen weitestgehend durch das Tonwählverfahren abgelöst worden.

Quellcode: Als Quellcode wird der Programmtext einer beliebigen Programmiersprache bezeichnet. Der Quellcode selbst kann keine Aktionen auslösen, da er zunächst kompiliert werden muss. Wenn der Quellcode eines Programms (z.B. eines Virus) verfügbar wird, können sehr leicht Varianten entwickelt werden.

Quicktime: Quicktime ist der Multimedia-Player von Apple.

RADIUS: Beim Remote Dial-In User Service kommunizieren Anwender und Server nicht nur verschlüsselt miteinander auch die Benutzerdaten werden verschlüsselt gespeichert.

RAID: Redundant Array of Inexpensive Disks ist eine Technologie die, die Zugriffsgeschwindigkeit oder die Datensicherheit auf Servern mit mehreren Festplatten dadurch erhöht, dass die einzelnen Festplatten gemeinsam einen Datenblock bearbeiten.

RAID 0: Bei RAID 0 (Striping) werden Datensicherheit und Zugriffsgeschwindigkeit ebenfalls durch die Verbindung mehrere Festplatten zu einer Arbeitseinheit erhöht. Allerdings werden die Datenblöcke nicht linear sondern parallel auf den verschiedenen Festplatten abgearbeitet. Dazu teilt sich der Datenblock zu gleichen Teilen auf die Festplatten auf. Mit dem Ausfall einer Festplatte ist bei RAID 0 allerdings zwanghaft der Verlust von Daten verbunden.

RAID 1: Im Fall von RAID 1 (Mirroring) werden die gleichen Daten parallel auf zwei Festplatten geschrieben. Dadurch steigert RAID 1 die Datensicherheit, denn auch bei Ausfall der einen Festplatten, kann problemlos auf die zweite Festplatte gewechselt und weitergearbeitet werden.

RAID 4: Wie RAID 0 werden auch bei RAID 4 die Informationen auf die unterschiedlichen Festplatten aufgeteilt. Allerdings wird bei RAID 4 eine Festplatte dazu benutzt Paritätsinformationen zu speichern. So können auch beim Ausfall einer Festplatte die Informationen aus den gespeicherten Paritätsinformationen wieder aufbereitet werden und gehen nicht verloren.

RAID 5: Bei RAID 5 (Parity Striping) werden wie bei RAID 4 Paritätsinformationen gespeichert. Jedoch nicht auf einer einzigen Festplatte, sondern verteilt auf unter-

schiedliche. Beim Ausfall einer Festplatte wird der Zugriff auf Paritätsinformationen dadurch im Vergleich zum RAID 4 beschleunigt.

Raubkopie: Eine Raubkopie ist eine nicht lizenzierte, nicht genehmigte Kopie eines Programms, die illegal von einem Originalprodukt angefertigt wurde. Jegliches Besitzen oder Anfertigen einer Raubkopie ist nach dem Urheberrecht strafbar.

Red Book: Als Red Book wird die Standard-Definition für das Format von Musik-CDs bezeichnet.

Redundant Array of Inexpensive Disks: Redundant Array of Inexpensive Disks ist eine Technologie, die die Zugriffsgeschwindigkeit oder die Datensicherheit auf Servern mit mehreren Festplatten dadurch erhöht, dass die einzelnen Festplatten gemeinsam einen Datenblock bearbeiten.

Registry: Registrierdatenbank in Windows, die zahlreiche für das Betriebssystem und installierte Anwendungen wichtige Einstellungen enthält. Sie können Sie editieren, indem Sie im Start-Menü „Ausführen“ wählen und dort „regedit“ eintippen. Achtung: Erstellen Sie vor Änderungen eine Sicherungskopie Ihrer Registrierdatenbank.

Re-Mailer: Ein Re-Mailer ist ein Server, der E-Mails anonymisiert weitersendet. Er entfernt alle persönlichen Informationen (Absenderadresse) und verschickt die Nachricht weiter. Normalerweise werden auf diesen Servern keine Daten über eingegangene E-Mails gespeichert.

Remote Dial-In User Service: Beim Remote Dial-In User Service kommunizieren Anwender und Server nicht nur verschlüsselt miteinander, auch die Benutzerdaten werden verschlüsselt gespeichert.

Reply: engl. Antwort. Antwort auf eine E-Mail oder eine andere elektronische Nachricht.

Request for Comments: Als Request For Comment (engl. Bitte um Kommentare) bezeichnet man Entwürfe und Arbeitspapiere, die öffentlich z.B. in Mailinglisten besprochen werden.

RFC: Als Request For Comment (engl. Bitte um Kommentare) bezeichnet man Entwürfe und Arbeitspapiere, die öffentlich z.B. in Mailinglisten besprochen werden.

RFID: RFID bezeichnet ein Verfahren zum Auslesen und Speichern von Daten per Funk. Ein Chip, der kleiner als ein Streichholzkopf ist, wird als Etikett auf eine Ware geklebt. Er beinhaltet eine Spule, die ein Magnetfeld erzeugt, und eine Antenne. Ein aktiver RFID Chip - man spricht auch von RFID Chip oder Smart Label - hat eine eigene Stromversorgung und kann weiter senden als ein passiver. Die Reichweiten liegen zwischen wenigen Zentimetern und einigen Hundert Metern. Sobald ein RFID Chip in die Nähe eines Lese-/Schreibgerätes kommt, sendet er die gespeicherten Informationen (aktuell zw. 1 Bit und 256 KBit) und speichert neue oder ändert vorhandene Informationen. Dieses Verfahren ermöglicht große Einsparungen im Bereich der Logistik. Daher drängen Großhändler wie Metro, Wal-Mart und Tesco auf die Einführung der Chips. Aber auch Ermittlungsbehörden und

Marktforschungsinstitute profitieren vom gläsernen Bürger bzw. Kunden. So stellen sie eine große Herausforderung für den Datenschutz dar.

RFID Tag: Als RFID Tag bzw. Smart Label bezeichnet man Funk-Etiketten, die kleiner als ein Streichholzkopf sind. Auf ihnen kann man Informationen wie z.B. den Electronic Product Code (EPC) speichern. Wegen ihrer geringen Größe kann man sie auf fast allen Gütern des täglichen Bedarfs anbringen. Man unterscheidet aktive und passive RFID Tags. Die aktiven haben eine eigene Stromversorgung und können daher über weite Entfernungen (> 1 km) von Lesegeräten erkannt werden und von Satelliten geortet werden. Passive RFID Tags haben keine eigene Stromversorgung, wodurch sie sehr preisgünstig herzustellen sind (Zielpreis: 1-2 Cent pro Chip). Ihre Reichweite ist auf wenige Meter beschränkt.

Rich Text Format: RTF steht für Rich Text Format. Dieses Textformat wurde von der Firma Microsoft für den Ex- und Import von Texten entwickelt.

RIP: Mit Hilfe des Routing Information Protocol haben Router die Möglichkeit untereinander Routingtabellen auszutauschen.

RIPE: Die „Réseaux IP Européenne“ regelt die Vergabe europäischer IP-Adressen.

Robot: Robots sind Programme, die in Datenbanken, Servern oder dem Internet relativ autonom bestimmte Aufgaben ausführen. Z.B. verwenden Suchmaschinen Robots, um die Inhalte von Webseiten für die Suchanfragen zu erfassen und zu indizieren.

Router: Als „Router“ werden Computer bezeichnet, die speziell für Routing-Aufgaben eingesetzt werden.

Routing: Der Transport von Daten innerhalb eines Netzes wird als „Routing“ bezeichnet. Als passives Routing wird der Transport von Daten innerhalb eines Netzes bezeichnet. Die für den Transport festgelegte Verbindung wird im Header der Daten definiert. Im Gegensatz zum passiven Routing ermittelt der Router beim aktiven Routing die kürzeste, schnellste, billigste oder nächstbeste Leitung aus der Routingtabelle. Dabei macht sich der ständige Austausch der Routingtabellen unter den Routern innerhalb eines Netzes besonders bezahlt.

Routing Information Protocol: Mit Hilfe des Routing Information Protocol haben Router die Möglichkeit untereinander Routingtabellen auszutauschen.

RTF: RTF steht für Rich Text Format. Dieses Textformat wurde von der Firma Microsoft für den Ex- und Import von Texten entwickelt.

Runtime error: Ein ‚run time error‘ (engl. Laufzeitfehler) ist ein Fehler, der auftritt, während ein Programm ausgeführt wird. Meist muss die Applikation nach einem Laufzeitfehler beendet werden. Im schlimmsten Fall muss der Rechner neu gebootet werden. Andere Fehler treten auf, wenn das Programm kompiliert (compile time error) wird.

S/MIME: Secure MIME ist ein DES basiertes Verfahren, das zum Verschlüsseln und elektronischen Unterschreiben von E-Mails genutzt wird.

SDK: Ein „Software Development Kit“ ist eine Sammlung von Bibliotheken, Schnittstellen und Tools, die es einem Entwickler erlauben fremde Software in seine Applikationen zu integrieren.

Secure Electronic Transaction: Das „Secure Electronic Transaction“-Protokoll dient der verschlüsselten Übertragung von Benutzerdaten übers Internet.

Secure Sockets Layer Protocol: Das Secure Sockets Layer-Protokoll bietet durch Datenver- und -entschlüsselung einen gesicherten Datenaustausch und wird oft für das Home-Banking genutzt.

Sektor, Festplatte: Ein Sektor ist die kleinste Einheit der Festplattenaufteilung (d.h. der kleinste adressierbare Teil eines Datenträgers). Ein Datenträger wird während der Formatierung in Sektoren aufgeteilt.

Serial Line Internet Protocol: Das „Serial Line Internet Protocol“ dient der Modemeinwahl in Computernetze. SLIP wurde inzwischen weitgehend durch das Point-to-Point Protocol (PPP) ersetzt.

Server: Als Server wird ein Programm bezeichnet, das einem Client Daten oder Dienste zur Verfügung stellt.

Server: Als Server werden Computer bezeichnet, die innerhalb eines Netzes (z.B. lokales Netzwerk oder auch über das Internet) Daten oder Dienste anderen Computern zur Verfügung stellen. Der G DATA-Server stellt Ihnen über das Internet-Update Virensignaturen zur ständigen Aktualisierung Ihrer Antivirensoftware zur Verfügung. Alternativ werden auch im Hintergrund laufende Programme, die Server-Aufgaben erfüllen, als „Server“ bezeichnet.

Server Message Block: SMB ist ein Protokoll, das in Windows zur Kommunikation zwischen Computern genutzt wird und Freigaben von Druckern, Dateien und Serial Ports regelt.

SET: Das „Secure Electronic Transaction“-Protokoll dient der verschlüsselten Übertragung von Benutzerdaten übers Internet.

SGML: In der Standard Generalized Markup Language werden die Grundlage aller Dokumentenbeschreibungssprachen wie HTML und XML festgelegt.

Short Messages Service: Der „Short Messages Service“ dient zur kostengünstigen und schnellen Versendung von Kurznachrichten auf Handys.

Simple Mail Transfer Protocol: Das Simple Mail Transfer Protocol ist ein Protokoll, dass den Versand von E-Mail steuert. Für den E-Mail-Empfang wird auf das POP3-Protokoll zurückgegriffen. Normalerweise wird für SMTP der Port 25 verwendet.

Site: Einzelne Internetseiten werden oft auch als „Site“ bezeichnet.

Slash: Der Slash (engl. Schrägstrich = „/“) ist ein Zeichen, das u.a. bei der Eingabe von Internetadressen und Verzeichnispfaden verwendet wird.

SLIP: Das „Serial Line Internet Protocol“ dient der Modemeinwahl in Computernetze. SLIP wurde inzwischen weitgehend durch das Point-to-Point Protocol (PPP) ersetzt.

Smart Label: Als RFID Tag bzw. Smart Label bezeichnet man Funk-Etiketten, die kleiner als ein Streichholzkopf sind. Auf ihnen kann man Informationen wie z.B. den Electronic Product Code (EPC) speichern. Wegen ihrer geringen Größe kann man sie auf fast allen Gütern des täglichen Bedarfs anbringen. Man unterscheidet

aktive und passive RFID Tags. Die aktiven haben eine eigene Stromversorgung und können daher über weite Entfernungen (> 1 km) von Lesegeräten erkannt werden und von Satelliten geortet werden. Passive RFID Tags haben keine eigene Stromversorgung, wodurch sie sehr preisgünstig herzustellen sind (Zielpreis: 1-2 Cent pro Chip). Ihre Reichweite ist auf wenige Meter beschränkt.

SMB: SMB ist ein Protokoll, das in Windows zur Kommunikation zwischen Computern genutzt wird und Freigaben von Druckern, Dateien und Serial Ports regelt.

SMS: Der „Short Messages Service“ dient zur kostengünstigen und schnellen Versendung von Kurznachrichten auf Handys.

SMTP: Das Simple Mail Transfer Protocol ist ein Protokoll, dass den Versand von E-Mail steuert. Für den E-Mail-Empfang wird auf das POP3-Protokoll zurückgegriffen. Normalerweise wird für SMTP der Port 25 verwendet.

Snail-Mail: Da der klassische Briefverkehr im Gegensatz zur E-Mail erheblich langsamer ist, wird er auch als Schneckenpost (engl. snail-mail) bezeichnet.

Sniffer: Sniffer sind Programme oder Personen, die den Datenverkehr abhören.

Social Engineering: Als Social Engineering werden Überredungstaktiken bezeichnet, mit denen ein Hacker einen Anwender dazu veranlasst Informationen preiszugeben, mit denen er dem Anwender oder seiner Organisation Schaden zufügen kann. Oft wird dazu Autorität vorgespiegelt, um Zugangsdaten oder Passwörter zu erlangen.

Software Development Kit: Ein „Software Development Kit“ ist eine Sammlung von Bibliotheken, Schnittstellen und Tools, die es einem Entwickler erlauben fremde Software in seine Applikationen zu integrieren.

Sourcecode: Als Quellcode wird der Programmtext einer beliebigen Programmiersprache bezeichnet. Der Quellcode selbst kann keine Aktionen auslösen, da er zunächst kompiliert werden muss. Wenn der Quellcode eines Programms (z.B. eines Virus) verfügbar wird, können sehr leicht Varianten entwickelt werden.

Spam: Mitte der 90er Jahre bezeichnet Spam die übermäßige Verbreitung der gleichen Nachricht in Usenet Foren. Der Begriff selbst geht auf einen Sketch von Monty Python zurück. Mittlerweile verwendet man Spam in mehreren Bedeutungen. Als Oberbegriff steht Spam für alle unaufgefordert zugesandten E-Mails. In einem engeren Sinne beschränkt sich der Begriff Spam auf WerbE-Mails; d.h. Würmer, Hoaxes, Phishing-Mails und AutoResponder werden nicht dazugezählt.

Spammer: Jemand, der Spam versendet.

Spyware: Als Spyware bezeichnet man Software, die Aktivitäten und Prozesse auf einem Rechner aufzeichnet und Fremden ohne Wissen und/oder Einverständnis des Besitzers zugänglich macht. Oft wird Spyware verwendet, um für Werbeeinblendungen das Surfverhalten zu analysieren, oder um Zugangsdaten für Bank- oder Online-Accounts zu erschnüffeln.

SQL: Die Structured Query Language erlaubt die Abfrage, Erzeugung und Änderung von Datenbanken und Datenbankeinträgen. Im Internet werden die

Ergebnisse der Datenbanksuche oft in HTML-Seiten angezeigt. Der verbreitetste Dialekt von SQL ist MySQL.

SSL: Das Secure Sockets Layer-Protokoll bietet durch Datenver- und -entschlüsselung einen gesicherten Datenaustausch und wird oft für das Home-Banking genutzt.

Standard Generalized Markup Language: In der Standard Generalized Markup Language werden die Grundlage aller Dokumentenbeschreibungssprachen wie HTML und XML festgelegt.

Stealth Viren: Stealth-Viren oder Tarnkappen-Viren besitzen spezielle Schutzmechanismen, um sich einer Entdeckung durch Virensuchprogramme zu entziehen. Dazu übernehmen sie die Kontrolle über verschiedene Systemfunktionen. Ist dieser Zustand erst einmal hergestellt, so können diese Viren beim normalen Zugriff auf Dateien oder Systembereiche nicht mehr festgestellt werden. Sie täuschen dem Virensuchprogramm einen nicht infizierten Zustand einer infizierten Datei vor. Die Tarnmechanismen von Stealth-Viren wirken erst, nachdem der Virus im Arbeitsspeicher resident geworden ist. Einige Viren benutzen Teilfunktionen von echten Stealth-Viren.

Steganografie: Über die Steganographie werden geheime Daten innerhalb anderer Daten versteckt werden. So kann man z.B. in Grafiken Textbotschaften verbergen oder Bilddaten in einer Soundfile.

Structured Query Language: Die Structured Query Language erlaubt die Abfrage, Erzeugung und Änderung von Datenbanken und Datenbankeinträgen. Im Internet werden die Ergebnisse der Datenbanksuche oft in HTML-Seiten angezeigt. Der verbreitetste Dialekt von SQL ist MySQL.

Subdomain: Eine Subdomain ist ein untergeordneter Teil einer Domain.

Subject: Das Subject ist die Betreffzeile einer E-Mail. Sie befindet sich im Header einer Nachricht.

SysOp: Als System Operator bezeichnet man den Administrator eines Rechnernetzwerks. Im Sinne eines Verwalters ist der Administrator für den korrekten Betrieb des Netzwerks zuständig.

Tab: Als Tab bezeichnet man eine Registerkarte oder ein Tabellenblatt, das es erlaubt in einem Programmfenster zwischen unterschiedlichen Inhalten umzuschalten. Tabellenblätter sind in Tabellenkalkulationsprogrammen wie Excel schon lange üblich. Seit kurzem gibt es auch viele Browser und Browseroberflächen, die es ermöglichen die Inhalte von mehreren Webseiten, in jeweils einem eigenen Tab anzuzeigen. Man spricht dann von Tabbed Browsing.

Tabbed Browsing: Als Tab bezeichnet man eine Registerkarte oder ein Tabellenblatt, das es erlaubt in einem Programmfenster zwischen unterschiedlichen Inhalten umzuschalten. Tabellenblätter sind in Tabellenkalkulationsprogrammen wie Excel schon lange üblich. Seit kurzem gibt es auch viele Browser und Browseroberflächen, die es ermöglichen die Inhalte von mehreren Webseiten, in jeweils einem eigenen Tab anzuzeigen. Man spricht dann von Tabbed Browsing.

TAPI: Als Telephony API wird eine von Microsoft entwickelte Programmierschnittstelle bezeichnet, die es Entwicklern ermöglicht auf die Funktionen von TAPI-konformen Modems zuzugreifen.

Taskleiste: Die Task- oder Startleiste von Microsoft Windows befindet sich voreingestellt am unteren Bildrand des Bildschirmhintergrunds (Desktop) und enthält links den „Start“-Button, über den Sie Programme und Einstellungen aufrufen können. Auf der rechten Seite des Balkens finden Sie neben der Systemuhr, Symbole von aktiven Programmen. Dies kann z.B. die Lautstärkeregelung Ihrer Soundkarte sein, aber z.B. auch der Antivirus-Virenwächter. Durch Anklicken des Symbols mit der linken oder rechten Maustaste können Sie hier weitere Einstellungen vornehmen.

TCP/IP: Die beiden Protokolle Transmission Control Protocol/Internet Protocol sind für die Adressierung und Weiterleitung von Daten im Netzwerk zuständig. Sie werden für die Kommunikation zwischen Computern mit unterschiedlichen Betriebssystemen eingesetzt. Sie entsprechen den Schichten 3 und 4 im OSI-Schichtenmodell.

Telnet: Mit Telnet wird ein Internet-Dienst bezeichnet, der dem Benutzer die Möglichkeit bietet sich auf einem Server einzuloggen, der dann vom Benutzer über bestimmte Befehle gesteuert werden kann. Ein Fenster präsentiert dem Benutzer das Bild des angewählten Rechners. Die Steuerung des Programms läuft über die eigene Tastatur, die dabei vom entfernten Rechner behandelt wird als sei sie direkt mit ihm verbunden.

Terminal: „Terminals“ stellten während der Großrechner-Ära über eine Kombination von Tastatur und Bildschirm eine Verbindung zum Großrechner her. Heute simuliert ein Terminalprogramm eine ähnliche Funktion, beispielsweise als Verbindung zu einer Mail-Box. Dementsprechend kann auch Telnet als eine Art Terminalprogramm bezeichnet werden.

Thumbnail: Als Thumbnails bezeichnet man kleine Kopien von Bilddateien in der Größe eines Daumennagels. Sie werden als Vorschaubilder in großen Bildersammlungen genutzt.

TLD: Die einzelnen Bestandteile einer Webadresse sind durch Punkte voneinander getrennt. Die Top Level Domain bezeichnet den letzten Teil der Adresse. In www.Antiviruslab.com wäre es „.com“. Die Top Level Domain stellt die oberste Ebene der Namensauflösung dar. Überregional gültige TLDs sind: .com (weltweite, kommerzielle Firmen), .mil (Militär), .gov (US-Regierung), .org (nicht-kommerzielle Organisationen), .edu (amerikanische Bildungseinrichtungen), .net (Netzverwaltungseinrichtungen), .int (internationale Behörden), .info, .museum, .name (natürliche Personen), .coop (Kooperationen), .aero (Luftfahrtorganisationen). Andere Top Level Domains sind nur für einzelne Länder gültig. Die Kennung enthält eine Kombination von 2 Buchstaben. Hier die bekanntesten: .de (Deutschland), .at (Österreich), .ch (Schweiz), .fr (Frankreich), .nl (Niederlande), .pl (Polen), .es (Spanien), .ca (Kanada).

Top Level Domain: Die einzelnen Bestandteile einer Webadresse sind durch Punkte voneinander getrennt. Die Top Level Domain bezeichnet den letzten Teil der Adresse. In www.Antivirustlab.com wäre es „.com“. Die Top Level Domain stellt die oberste Ebene der Namensauflösung dar. Überregional gültige TLDs sind: .com (weltweite, kommerzielle Firmen), .mil (Militär), .gov (US-Regierung), .org (nicht-kommerzielle Organisationen), .edu (amerikanische Bildungseinrichtungen), .net (Netzverwaltungseinrichtungen), .int (internationale Behörden), .info, .museum, .name (natürliche Personen), .coop (Kooperationen), .aero (Luftfahrtorganisationen). Andere Top Level Domains sind nur für einzelne Länder gültig. Die Kennung enthält eine Kombination von 2 Buchstaben. Hier die bekanntesten: .de (Deutschland), .at (Österreich), .ch (Schweiz), .fr (Frankreich), .nl (Niederlande), .pl (Polen), .es (Spanien), .ca (Kanada).

Traceroute: Als Traceroute wird ein Tool bezeichnet, das alle Server aufzeichnet, die ein IP-Paket während seiner Reise durchs Internet durchläuft.

Transmission Control Protocol/ Internet Protocol: Die beiden Protokolle Transmission Control Protocol/Internet Protocol sind für die Adressierung und Weiterleitung von Daten im Netzwerk zuständig. Sie werden für die Kommunikation zwischen Computern mit unterschiedlichen Betriebssystemen eingesetzt. Sie entsprechen den Schichten 3 und 4 im OSI-Schichtenmodell.

Transponder: Der Begriff Transponder ist aus den englischen Ausdrücken Transmitter (Sender) und Responder (Antwörter) zusammengesetzt. Technisch definiert ist ein Transponder ein oft kabelloses Gerät, das eingehende Signale aufnimmt und automatisch darauf antwortet. Dabei können auch Daten gespeichert und verändert werden. Transponder werden eingesetzt, um Flugzeuge im Luftverkehr zu identifizieren, zum Diebstahlschutz in Kaufhäusern oder Tiere bekommen ihn unter in Glaskugeln unter die Haut injiziert, um den Transportweg lückenlos verfolgen zu können. Auch die umstrittenen RFID Tags sind Transponder.

Trojaner: Der Name Trojanisches Pferd ist angelehnt an das geschichtliche Vorbild und beschreibt ein Programm, das dem Anwender vorgibt, eine bestimmte und gewollte Funktion zu besitzen. Zusätzlich dazu beinhalten Trojaner jedoch noch einen versteckten Programmteil, der gleichsam eine Hintertür zum befallenen Rechner öffnet und so nahezu vollen Zugriff auf das betroffene System gewährt ohne, dass der Benutzer dies bemerkt. Die Methoden von Trojanern, sich zu verstecken sind dabei schier unbegrenzt, so werden diese heimtückischen Programme oftmals als Bildschirmschoner oder Spiele per E-Mail verschickt. Ein einmaliges Starten genügt bereits und der Schädling infiziert das System.

Trojanisches Pferd: Der Name Trojanisches Pferd ist angelehnt an das geschichtliche Vorbild und beschreibt ein Programm, das dem Anwender vorgibt, eine bestimmte und gewollte Funktion zu besitzen. Zusätzlich dazu beinhalten Trojaner jedoch noch einen versteckten Programmteil, der gleichsam eine Hintertür zum befallenen Rechner öffnet und so nahezu vollen Zugriff auf das betroffene System gewährt ohne, dass der Benutzer dies bemerkt. Die Methoden von Trojanern, sich zu verstecken sind dabei schier unbegrenzt, so werden diese heimtückischen

Programme oftmals als Bildschirmschoner oder Spiele per E-Mail verschickt. Ein einmaliges Starten genügt bereits und der Schädling infiziert das System.

TSAPI: Telephony Server API ist ein Produkt, das von den amerikanischen Unternehmen Novell und AT&T entwickelt wurde um mit TAPI konkurrieren zu können. Bedingung für den Gebrauch von TSAPI ist ein Novell Netware-Server, der über Telefonkabel mit der Außenwelt vernetzt sein muss.

Tunneling: Beim Tunneling werden Daten eines Protokolls in ein anderes Netzwerkprotokoll eingebettet. So können sichere (verschlüsselte) Verbindungen (wie SSH) über ungesicherte Netzwerke (TCP/IP, SMTP) aufgebaut werden. Ein Tunnel kann auch dazu genutzt werden, um eine Firewall zu umgehen. Mit einem ausgehenden Tunnel kann ein Nutzer aus dem Intranet auf externe Rechner, Netze oder Dienste zugreifen. Bei eingehenden Tunnels, kann ein externer Nutzer auf einen Dienst, Rechner oder Daten des Intranet zugreifen.

UART: Als Universal Asynchronous Receiver/Transmitter bezeichnet man einen Baustein der die asynchrone Datenübertragung ermöglicht. Wegen seines Fifos ist der UART für schnelle Verbindungen unerlässlich.

UCE: Unsolicited E-Mail stellt ein Synonym zu Spam dar und ist daher ebenfalls eine Bezeichnung für unerwünschte E-Mails.

Uniform Resource Identifier: Der Uniform Resource Identifier (URI) ist der Oberbegriff für eine Zeichenfolge, die eine Ressource (in einem Rechner) eindeutig bestimmt. Man kann URIs auch als Namen ansehen, wobei diese allerdings im Gegensatz zu Namen bei Menschen genau einmal vorkommen. URIs werden meist verwendet, um Webseiten, Webdienste oder E-Mail-Empfänger im Internet zu bezeichnen.

Uniform Resource Locator: Der „Uniform Resource Locator“ ist vereinfacht gesagt die Adresse einer Datei (Text, Grafik, Software, o.ä.) im Internet. Ein URL ist eigentlich ein Sonderfall eines URI und setzt sich aus folgenden Teilen zusammen: 1. Das Protokoll (z.B. http, https, ftp, news, gopher) gefolgt von einem Doppelpunkt und zwei Schrägstrichen „://“ 2a. ggf. ein Benutzername und ein Passwort, durch einen Doppelpunkt „:“ getrennt und mit einem Klammeraffen „@“ abgeschlossen. 2b. Der Hostname (entweder als Domain oder als IP-Adresse) gefolgt von einem Schrägstrich „/“ 3. Verzeichnispfad getrennt durch Schrägstriche „/“ 4. Dateiname 5. ggf. Parameter für die Datei. Mit einem Fragezeichen „?“ wird der Beginn des Parameterblocks gekennzeichnet. Mehrere Parameter werden durch ein Handelskammer-Und „&“ voneinander getrennt. Z.B.: <http://user:passwort@www.gdata.de/trade/productview/472/index.php?param1=0&param2=1>

Universal Asynchronous Receiver/Transmitter: Als Universal Asynchronous Receiver/Transmitter bezeichnet man einen Baustein der die asynchrone Datenübertragung ermöglicht. Wegen seines Fifos ist der UART für schnelle Verbindungen unerlässlich.

Universal Serial Bus: Der „Universal Serial Bus“ ermöglicht den Anschluss peripherer Geräte wie Datenspeicher, Maus oder Drucker an den PC auch während das System in Betrieb ist.

Update: Mit dem Begriff „Update“ werden Aktualisierungen von Datenmaterial und Programmen (z.B. Software, Antivirendaten, Datenbanken) bezeichnet. Bei G DATA AntiVirus haben Sie die Möglichkeit, die Antivirensignaturen regelmäßig via Internet zu aktualisieren (Viren-Update). Aber auch die G DATA-AntiVirus-Software selbst können Sie auf den neuesten Stand zu bringen (Software-Update).

Upgrade: Der Begriff Upgrade steht in enger Verbindung zum Begriff Update. Allerdings bezieht sich das Upgrade auf die Aufrüstung der Hardware des PC.

Upload: Upload bezeichnet das Gegenteil von Download. Dabei werden Daten vom eigenen Rechner an einen anderen geschickt. Wenn z.B. Dateien für einen Webserver vom lokalen Rechner auf den Webserver übertragen werden, spricht man von einem Upload.

URI: Der Uniform Ressource Identifier (URI) ist der Oberbegriff für eine Zeichenfolge, die eine Ressource (in einem Rechner) eindeutig bestimmt. Man kann URIs auch als Namen ansehen, wobei diese allerdings im Gegensatz zu Namen bei Menschen genau einmal vorkommen. URIs werden meist verwendet, um Webseiten, Webdienste oder E-Mail-Empfänger im Internet zu bezeichnen.

URL: Der „Uniform Ressource Locator“ ist vereinfacht gesagt die Adresse einer Datei (Text, Grafik, Software, o.ä.) im Internet. Ein URL ist eigentlich ein Sonderfall eines URI und setzt sich aus folgenden Teilen zusammen: 1. Das Protokoll (z.B. http, https, ftp, news, gopher) gefolgt von einem Doppelpunkt und zwei Schrägstrichen „://“ 2a. ggf. ein Benutzername und ein Passwort, durch einen Doppelpunkt „:“ getrennt und mit einem Klammeraffen „@“ abgeschlossen. 2b. Der Hostname (entweder als Domain oder als IP-Adresse) gefolgt von einem Schrägstrich „/“ 3. Verzeichnispfad getrennt durch Schrägstriche „/“ 4. Dateiname 5. ggf. Parameter für die Datei. Mit einem Fragezeichen „?“ wird der Beginn des Parameterblocks gekennzeichnet. Mehrere Parameter werden durch ein Handelskammer-Und „&“ voneinander getrennt. Z.B.: <http://user:passwort@www.gdata.de/trade/productview/472/index.php?param1=0&param2=1>

USB: Der „Universal Serial Bus“ ermöglicht den Anschluss peripherer Geräte wie Datenspeicher, Maus oder Drucker an den PC auch während das System in Betrieb ist.

Usenet: Als „Usenet“ wird ein Computernetz bezeichnet, das zwar unabhängig vom Internet entstand, heute aber weitgehend über das Internet abgewickelt wird und dem Austausch von Mitteilungen sowie Meinungen in diversen Newsgroups dient. Das „USErs NETwork“ ist genaugenommen ein Diskussionsbrett, das auf speziellen News-Servern läuft. Als Transportmittel für die Nachrichten werden hierbei ganz unterschiedliche Netzwerke ebenso wie natürlich auch Teile des Internet benutzt. Im Usenet gibt es nur öffentlich zugängliche Nachrichten. Das heißt, dass auf eine einmal gepostete Nachricht beliebig viele Teilnehmer antworten können. Das führt oft zu langen und komplizierten Ketten von Rede und Gegenrede, die man Threads (engl. „Faden“) nennt.

User: Als User (engl. „Nutzer“) wird der Benutzer und Anwender eines ComputerSystems bezeichnet.

UUdecode: In den frühen Tagen der E-Mail war es nur möglich Dateien mit ASCII-Zeichen zu versenden. Binärdateien konnten also nicht übertragen werden. Das Kommandozeilenprogramm ‚UUencode‘ schaffte hier Abhilfe. Es konnte Binärdateien in ASCII-kompatible Zeichen umgewandeln. Diese konnten dann per E-Mail übertragen werden. Das Gegenstück ‚UUdecode‘ wandelt die ASCII Zeichen wieder zurück in Binärdaten. Die beiden ‚UU‘ stehen für ‚Unix-to-Unix‘ und zeugen vom ursprünglichen Zweck des Programms der sicheren Übertragung von Daten zwischen Unix-Rechnern.

UUencode: In den frühen Tagen der E-Mail war es nur möglich Dateien mit ASCII-Zeichen zu versenden. Binärdateien konnten also nicht übertragen werden. Das Kommandozeilenprogramm ‚UUencode‘ schaffte hier Abhilfe. Es konnte Binärdateien in ASCII-kompatible Zeichen umgewandeln. Diese konnten dann per E-Mail übertragen werden. Das Gegenstück ‚UUdecode‘ wandelt die ASCII Zeichen wieder zurück in Binärdaten. Die beiden ‚UU‘ stehen für ‚Unix-to-Unix‘ und zeugen vom ursprünglichen Zweck des Programms der sicheren Übertragung von Daten zwischen Unix-Rechnern.

UU-Kodierung: In den frühen Tagen der E-Mail war es nur möglich Dateien mit ASCII-Zeichen zu versenden. Binärdateien konnten also nicht übertragen werden. Das Kommandozeilenprogramm ‚UUencode‘ schaffte hier Abhilfe. Es konnte Binärdateien in ASCII-kompatible Zeichen umgewandeln. Diese konnten dann per E-Mail übertragen werden. Das Gegenstück ‚UUdecode‘ wandelt die ASCII Zeichen wieder zurück in Binärdaten. Die beiden ‚UU‘ stehen für ‚Unix-to-Unix‘ und zeugen vom ursprünglichen Zweck des Programms der sicheren Übertragung von Daten zwischen Unix-Rechnern.

VBScript: Als VBScript wird eine Skriptsprache bezeichnet, die auf der Programmiersprache Visual Basic aufbaut und von Microsoft als Ergänzung von HTML entwickelt wurde.

Viren, polymorphe: Polymorphe Viren enthalten Mechanismen, um ihr Aussehen bei jeder Infektion zu verändern. Dazu gehört unter anderem der Austausch von Befehlssequenzen und zufallsgesteuertes Einstreuen von unsinnigen Befehlsgruppen. Diese sind in keiner Weise für das Funktionieren des Virus erforderlich. So können leicht Milliarden von Varianten eines Virus entstehen. Um verschlüsselte und polymorphe Viren sicher zu erkennen und zu beseitigen, reicht der Einsatz klassischer Virensignaturen häufig nicht aus. Meist müssen spezielle Programme geschrieben werden. Der Aufwand zur Analyse und zur Bereitstellung geeigneter Gegenmittel kann dabei extrem hoch sein. So sind polymorphe Viren ohne Übertreibung als die Königsklasse unter den Viren zu bezeichnen.

Viren, Stealth: Stealth-Viren oder Tarnkappen-Viren besitzen spezielle Schutzmechanismen, um sich einer Entdeckung durch Virensuchprogramme zu entziehen. Dazu übernehmen sie die Kontrolle über verschiedene Systemfunktionen. Ist dieser Zustand erst einmal hergestellt, so können diese Viren beim normalen Zugriff auf Dateien oder Systembereiche nicht mehr festgestellt

werden. Sie täuschen dem Virensuchprogramm einen nicht infizierten Zustand einer infizierten Datei vor. Die Tarnmechanismen von Stealth-Viren wirken erst, nachdem der Virus im Arbeitsspeicher resident geworden ist. Einige Viren benutzen Teilfunktionen von echten Stealth-Viren.

Virensignatur: Ein sehr effektives Mittel zur Erkennung und Beseitigung von Viren ist der Vergleich der möglichen Viren mit der jeweiligen Virensignatur. Die Virensignatur ist im Prinzip eine Schablone, die genau auf einen Virus oder Virentyp passt und ihn auf diese Weise schnell erkennt. Da diese Schablonen erst dann erstellt werden können, wenn der Virus das erste Mal auftauchte und von Antivirenexperten analysiert wurde, ist es um so wichtiger, dass Sie möglichst immer die aktuellsten Virensignaturen auf Ihrem Computer zur Verfügung haben.

Virtual Network Computing: Durch „Virtual Network Computing“-Programme ist es möglich, einen Rechner von einem anderen Rechner fernzusteuern, so als ob man direkt davor sitzt. Mit VNC-Programmen wie TightVNC oder RealVNC können Systemadministratoren die Rechner des Netzwerks von Ihrem Arbeitsplatz aus warten und konfigurieren oder Privatanwender können den heimischen PC vom Rechner am Arbeitsplatz ansteuern. Der VNC-Server überträgt den Bildschirminhalt des ferngesteuerten PCs. Auf dem Rechner des SysAdmins sorgt der VNC-Viewer dafür, dass die lokalen Mausbewegungen und Tastaturbefehle an den entfernten Rechner übertragen werden. VNC wurde von AT&T und der University Cambridge entwickelt und ist plattformunabhängig nutzbar. Es kann sogar in Browser integriert werden.

Virtual Reality Modeling Language: Die Virtual Reality Modeling Language ist wie XML und HTML eine SGML-konforme, plattformunabhängige Beschreibungssprache für dreidimensionale virtuelle Welten.

Virtuell: Als virtuell wird eine Umgebung dann bezeichnet, wenn sie nicht auf dem realen Leben (RL engl. real life) basiert, sondern vom Computer generiert wird. Verwirrenderweise spricht man dann von virtueller Realität (VR).

Virtueller Speicher: Jeder Rechner enthält einen Speicherbereich, in dem die Daten, die gerade vom Rechner gebraucht werden abgelegt werden. Diesen Bereich nennt man RAM (Random Access Memory). Der Zugriff auf den RAM-Speicher ist viel schneller als der Zugriff auf die Festplatte. Die Größe des RAMs ist allerdings beschränkt (z.B. auf 256 MB). Wenn jetzt sehr viele und/oder große Dateien geöffnet sind, kann es vorkommen, dass nicht alle Dateien im RAM Platz haben. Dann wird ein Teil des RAMs auf die Festplatte ausgelagert - und zwar in die Auslagerungsdatei.

Virtual Server: Mit einem Virtual Server-System kann man durch die Zuordnung verschiedener IP-Adressen auf einem Computer mehrere Server simulieren.

Visit: Als Visit wird der Besuch einer Website durch einen Anwender bezeichnet, der anhand seiner IP-Adresse erkannt wird.

VNC: Durch „Virtual Network Computing“-Programme ist es möglich, einen Rechner von einem anderen Rechner fernzusteuern, so als ob man di-

rekt davor sitzt. Mit VNC-Programmen wie TightVNC oder RealVNC können Systemadministratoren die Rechner des Netzwerks von Ihrem Arbeitsplatz aus warten und konfigurieren oder Privatanwender können den heimischen PC vom Rechner am Arbeitsplatz ansteuern. Der VNC-Server überträgt den Bildschirminhalt des ferngesteuerten PCs. Auf dem Rechner des SysAdmins sorgt der VNC-Viewer dafür, dass die lokalen Mausbewegungen und Tastaturbefehle an den entfernten Rechner übertragen werden. VNC wurde von AT&T und der University Cambridge entwickelt und ist plattformunabhängig nutzbar. Es kann sogar in Browser integriert werden.

VRML: Die Virtual Reality Modeling Language ist wie XML und HTML eine SGML-konforme, plattformunabhängige Beschreibungssprache für dreidimensionale virtuelle Welten.

W3C: Das ‚World-Wide-Web Consortium‘ bildet einen Teil der ISOC. Seine Aufgabe ist, die Standards und Technologien festzusetzen, die im WWW Verwendung finden. Unter anderem entscheidet das WWW-Consortium welche Spezifikationen für Skriptsprachen gelten.

WAIS: Wide Area Information Server ist das älteste und mittlerweile veraltete Suchsystem für Informationen im Internet. Bevor die Volltextsuche mit den eigentlichen Schlüsselwörtern beginnt, müssen aus einer langen Liste von Datenbanken und Dokumentensammlungen die Datenquellen ausgewählt werden, die durchsucht werden sollen.

WAN: Als „Wide Area Network“ wird ein Computer-Netzwerk bezeichnet, das sich über eine größere Fläche erstreckt.

Wardriver: Als Wardriver bezeichnet man (böse) Menschen, die mit einem Laptop auf dem Beifahrersitz herumfahren und nach ungesicherten WLANs (kabellose Netzwerke) suchen. Sind sie fündig geworden surfen sie im günstigsten Fall auf Kosten des WLAN-Betreibers. Es ist aber auch möglich, dass ein Wardriver Zugang zu Dateien auf dem Netzwerk bekommt und diese stiehlt. So können die Urlaubsbilder, die Kundendaten oder die Datei mit Passwörtern in unbefugte Hände gelangen.

Warmstart: Neustart des Rechners, durch (längeres) Drücken der Reset-Taste. Im Gegensatz zum Kaltstart, können speicherresidente Viren einen Warmstart überdauern.

Warwalker: Siehe Wardriver. Im Gegensatz zum Wardriver sucht der Warwalker auf der Suche nach ungesicherten WLANs auf Schusters Rappen (d.h. zu Fuß).

Webmaster: Als „Webmaster“ wird der Verwalter eines Webangebots bezeichnet.

Webserver: Ein Server-Dienst, der Daten über das HTTP-Protokoll zur Verfügung stellt und über eine eindeutige HTTP-URL erreichbar ist. Oft wird auch der Rechner, auf dem der Server-Dienst läuft als Webserver bezeichnet. Meistens liefert ein Webserver HTML Dateien aus. Er stellt aber auch Grafiken, Stylesheets, und andere Date(i)en zur Verfügung.

Whois: In sog. Whois-Datenbanken werden Informationen zu Eigentümern und Betreibern von Domains gespeichert und über das gleichnamige Protokoll allen Internetnutzern zugänglich gemacht. So kann man z.B. herausfinden, in welchem Land der Server für eine bestimmte IP-Adresse steht und wer ihn angemeldet hat.

Wide Area Information Server: Wide Area Information Server ist das älteste und mittlerweile veraltete Suchsystem für Informationen im Internet. Bevor die Volltextsuche mit den eigentlichen Schlüsselwörtern beginnt, müssen aus einer langen Liste von Datenbanken und Dokumentensammlungen die Datenquellen ausgewählt werden, die durchsucht werden sollen.

Wide Area Network: Als „Wide Area Network“ wird ein Computer-Netzwerk bezeichnet, das sich über eine größere Fläche erstreckt.

WiFi: Wireless Fidelity ist eine Vereinigung von Unternehmen und Organisationen, die ursprünglich Wireless Ethernet Compatibility Alliance (WECA) hieß. Ziel der Organisation ist es Produkte aus dem Bereich kabelloses Netzwerk, die zwischen Ethernet und dem WLAN-Standard IEEE 802.11 vermitteln, auf Kompatibilität zu testen. Die Mitglieder vergeben für ihre Produkte ein kostenpflichtiges Prüfsiegel, sofern die Produkte den selbst erstellten Richtlinien entsprechen.

Windows NT LAN Manager: Der Microsoft Windows NT LAN Manager ist ein Protokoll, das beim Einloggen den Datentransfer zwischen Client, Server und Domain Controller gewährleistet. Es ist mittlerweile von Kerberos abgelöst und gilt als veraltet und nicht besonders sicher. Es wird nur noch aus Gründen der Abwärtskompatibilität mit Windows NT 4.0 (und früher) weiterhin unterstützt.

Wireless Fidelity: Wireless Fidelity ist eine Vereinigung von Unternehmen und Organisationen, die ursprünglich Wireless Ethernet Compatibility Alliance (WECA) hieß. Ziel der Organisation ist es Produkte aus dem Bereich kabelloses Netzwerk, die zwischen Ethernet und dem WLAN-Standard IEEE 802.11 vermitteln, auf Kompatibilität zu testen. Die Mitglieder vergeben für ihre Produkte ein kostenpflichtiges Prüfsiegel, sofern die Produkte den selbst erstellten Richtlinien entsprechen.

Wireless LAN: Ein Wireless LAN bezeichnet ein kabelloses, lokales Netzwerk, das per Funk betrieben wird. Die meisten lokalen Funknetze basieren auf den Standards „IEEE 802.11“ oder „HIPERLAN“, die zwei Betriebsarten unterstützen: 1. über einen „Wireless Access Point“ (WAP), der die einzelnen Netzwerkknoten koordiniert und den Zugang zu externen Netzen ermöglicht. 2. Alle Rechner sind gleichberechtigt, wodurch zwar ein Datenaustausch aber keine Verbindung in externe Netze möglich ist. In IEEE 802.11-konformen Funknetzen können bei der Übertragung Verschlüsselungsverfahren angewendet werden, die aber nicht mehr dem aktuellen Stand der Technik entsprechen. Der Standard IEEE 802.11i schafft hier Abhilfe. Leider sind viele WLANs ungeschützt, wie der jährliche auf www.worldwidewardrive.org gezeigt wird.

Wireless Local Area Network: Ein Wireless LAN bezeichnet ein kabelloses, lokales Netzwerk, das per Funk betrieben wird. Die meisten lokalen Funknetze basieren auf

den Standards „IEEE 802.11“ oder „HIPERLAN“, die zwei Betriebsarten unterstützen: 1. über einen „Wireless Access Point“ (WAP), der die einzelnen Netzwerkknoten koordiniert und den Zugang zu externen Netzen ermöglicht. 2. Alle Rechner sind gleichberechtigt, wodurch zwar ein Datenaustausch aber keine Verbindung in externe Netze möglich ist. In IEEE 802.11-konformen Funknetzen können bei der Übertragung Verschlüsselungsverfahren angewendet werden, die aber nicht mehr dem aktuellen Stand der Technik entsprechen. Der Standard IEEE 802.11i schafft hier Abhilfe. Leider sind viele WLANs ungeschützt, wie der jährliche auf www.worldwidewardrive.org gezeigt wird.

WLAN: Ein Wireless LAN bezeichnet ein kabelloses, lokales Netzwerk, das per Funk betrieben wird. Die meisten lokalen Funknetze basieren auf den Standards „IEEE 802.11“ oder „HIPERLAN“, die zwei Betriebsarten unterstützen: 1. über einen „Wireless Access Point“ (WAP), der die einzelnen Netzwerkknoten koordiniert und den Zugang zu externen Netzen ermöglicht. 2. Alle Rechner sind gleichberechtigt, wodurch zwar ein Datenaustausch aber keine Verbindung in externe Netze möglich ist. In IEEE 802.11-konformen Funknetzen können bei der Übertragung Verschlüsselungsverfahren angewendet werden, die aber nicht mehr dem aktuellen Stand der Technik entsprechen. Der Standard IEEE 802.11i schafft hier Abhilfe. Leider sind viele WLANs ungeschützt, wie der jährliche auf www.worldwidewardrive.org gezeigt wird.

World Wide Web: Das WWW wurde 1981 von Tim Berners-Lee am CERN entwickelt. Es ist eine Art „Unternetz“ des Internet, das von WWW-Servern gebildet wird, die Daten über bestimmte Transfer Protokolle (wie z.B. HTTP) zum Abruf bereitstellen. Im Gegensatz zur früheren reinen Textdarstellung im Internet bietet das WWW die Möglichkeit, Textinformationen, Grafiken, Töne, Animationen, Virtuelle 3D Welten und sogar Videos im Internet zu übertragen. Eine weitere Kernfunktion ist der Einsatz von Hyperlinks, die das schnelle Springen zu verwandten Sites im WWW erlauben. Um sich im WWW zu bewegen, ist außer der Internet-Verbindung ein WWW-Browser notwendig. Das WWW verdrängte Bulletin Boards und Gopher fast vollständig und wurde zum Informationsträger Nummer 1. Viele Anwender die vom Internet sprechen, meinen eigentlich das WWW.

World Wide Web Consortium: Das ‚World-Wide-Web Consortium‘ bildet einen Teil der ISOC. Seine Aufgabe ist, die Standards und Technologien festzusetzen, die im WWW Verwendung finden. Unter anderem entscheidet das WWW-Consortium welche Spezifikationen für Skriptsprachen gelten.

WWW: Das WWW wurde 1981 von Tim Berners-Lee am CERN entwickelt. Es ist eine Art „Unternetz“ des Internet, das von WWW-Servern gebildet wird, die Daten über bestimmte Transfer Protokolle (wie z.B. HTTP) zum Abruf bereitstellen. Im Gegensatz zur früheren reinen Textdarstellung im Internet bietet das WWW die Möglichkeit, Textinformationen, Grafiken, Töne, Animationen, Virtuelle 3D Welten und sogar Videos im Internet zu übertragen. Eine weitere Kernfunktion ist der Einsatz von Hyperlinks, die das schnelle Springen zu verwandten Sites im WWW erlauben. Um sich im WWW zu bewegen, ist außer der Internet-Verbindung ein

WWW-Browser notwendig. Das WWW verdrängte Bulletin Boards und Gopher fast vollständig und wurde zum Informationsträger Nummer 1. Viele Anwender die vom Internet sprechen, meinen eigentlich das WWW.

WYSIWYG: WYSIWYG ist ein Akronym für „What You See Is What You Get“ (Was Du siehst, ist was Du bekommst). Der Begriff wurde in den frühen Tagen des Web-Publishing geprägt. Damals unterschied sich die Darstellung im (oft textbasierten) Editor stark von der Anzeige im Browser. Mit WYSIWYG war die Darstellung im Editor identisch mit der im Browser.

X-Modem: X-Modem ist eines der ältesten Protokolle. Mit Hilfe eines Modems überträgt es Daten zwischen zwei PCs.

XSS: Eine Sicherheitslücke, bei der Skripte von einer Webseite in einer anderen Webseite ausgeführt werden. Der Nutzer merkt nicht, dass ein fremdes Skript ausgeführt wird, da sich die angezeigte URL-Adresse nicht ändert.

Y-Modem: Y-Modem erweitert das X-Modem-Protokoll. Es ermöglicht zusätzlich die Übertragung von Dateinamen, Dateigröße und die Batch-Übertragungen.

ZIP: ZIP ist ein Dateiformat, das es ermöglicht, mehrere Dateien auch mit Unterverzeichnissen zu einem Archiv zusammenzufassen. Die im Archiv enthaltenen Dateien werden einzeln komprimiert. So lassen sie sich später auch einzeln wieder extrahieren. Das ZIP-Format wurde 1989 von Phil Katz als Public Domain Software entwickelt und mit den Programmen PKZIP und PKUNZIP verbreitet. Mittlerweile hat sich ‚ZIP‘ zum Synonym für ein komprimiertes Archiv entwickelt und kann von vielen anderen Packprogrammen verarbeitet werden.

Z-Modem: Als Z-Modem wird ein inzwischen veraltetes Protokoll bezeichnet, das die Kommunikation zwischen zwei Computern ermöglicht. Z-Modem wird nach wie vor genutzt, weil es die Fähigkeit besitzt, die Größe der zu übertragenden Datei, der Leitungsqualität dynamisch anzupassen.

Zombie-PC: Als Zombie bezeichnet man einen PC, der über eine Backdoor fernsteuerbar ist. Analog zum filmischen Vorbild gehorcht der Zombie-PC nur noch dem verborgenen Master und führt dessen oftmals verbrecherische Befehle aus. Meist werden viele Zombies zu sogenannten Botnetzen zusammengefasst.

Zooviren: Viren, die nur beim ‚Virenautor‘ und in einschlägigen Virensammlungen (z.B. bei Virensammlern, Hersteller von Antivirensoftware oder Testern) zu finden sind, nennt man Zoo-Viren. Diese Viren tauchen nie beim Anwender, also ‚in the wild‘ auf.

Zugriffsrechte: Die Zugriffsrechte werden innerhalb eines Computersystems vom Administrator an den Nutzer vergeben, um den Handlungsspielraum des Nutzers genau zu definieren.

■ Virenkategorien

Wenn von Viren, Würmern und Trojanischen Pferden gesprochen wird, ist damit im Allgemeinen ein schädlicher Aspekt von Software verbunden. Als Oberbegriff dafür hat sich der Begriff Malware (von malicious = boshaft, schädlich und Software) durchgesetzt. Unter Malware werden Programme zusammengefasst, die in böser Absicht elektronische Daten zugänglich machen, verändern oder löschen. Malware besitzt immer eine Schadensfunktion (engl. Payload) und verursacht unterschiedliche Effekte. Dies kann von eher harmlosen Bekundungen des eigenen Vorhandenseins über ausspionieren von persönlichen Daten bis hin zur Löschung der Festplatte reichen. Malware kann man in die 3 Gruppen Trojanische Pferde, Würmer und Viren untergliedern. In einem erweiterten Sinn fallen auch Spyware und Dialer darunter.

■ Trojaner

Trojaner unterscheiden sich von Würmern und Viren dadurch, dass sie sich nicht selbsttätig reproduzieren. Der Name Trojanisches Pferd ist angelehnt an das geschichtliche Vorbild und beschreibt ein Programm, das dem Anwender vorgibt, eine bestimmte und gewollte Funktion zu besitzen. Zusätzlich dazu beinhalten Trojaner jedoch noch einen versteckten Programmteil, der gleichsam eine Hintertür zum befallenen Rechner öffnet und so nahezu vollen Zugriff auf das betroffene System gewähren kann ohne, dass der Benutzer dies bemerkt. Die Methoden von Trojanern, sich zu verstecken sind dabei schier unbegrenzt. Sie können sich in Kommandozeilenbefehlen für UNIX-Systemadministratoren wie passwd, ps, netstat verstecken (sog. Rootkits) oder als Remote Access Trojans (sog. RATs, auch Backdoor genannt) daherkommen. Diese heimtückischen Programme werden aber auch als Bildschirmschoner oder Spiele per E-Mail verschickt. Ein einmaliges Starten genügt bereits und der Schädling infiziert das System.

■ Gemeinsamkeiten von Viren und Würmern

Viren und Würmer sind aus folgenden Teilen aufgebaut:

Reproduktionsteil: Mit diesem Programmteil wird die Vermehrung des Virus durchgeführt. Dieser Teil ist obligatorisch für alle Viren. Die Infektion kann über Disketten (und andere wechselbare Datenträger), freigegebene Ordner, Netzwerkscans, Peer-to-Peer Netzwerke oder E-Mail erfolgen. Dabei nutzen die Schädlinge viele verschiedene Angriffspunkte, die teilweise nur auf bestimmten Kombinationen von Hardware, Software und Betriebssystem funktionieren.

Erkennungsteil: Im Erkennungsteil wird geprüft, ob schon eine Infektion mit diesem Virus vorliegt. Jedes Wirts-Programm wird nur einmal infiziert, um die Verbreitung zu beschleunigen und die Tarnung aufrecht zu erhalten.

Schadensteil: Die Schadensfunktionen (engl. Payload), die mit Viren und Würmern einhergehen kann man in folgende Gruppen einordnen:

- Mit **Backdoor**-Programmen verschafft sich der Hacker Zugang zum Rechner und den Daten und kann so Daten manipulieren oder Denial of Service Attacken starten.
- Es können Datenmanipulationen vorgenommen werden. Das reicht von (mehr oder weniger lustigen) Meldungen, Anzeigen und Geräuschen bis hin zum Löschen von Dateien und Laufwerken.
- Es können auch Informationen ausgespäht und versendet werden. Ziel dieser Attacken sind Passwörter, Kreditkartennummern, Loginnamen und andere persönliche Daten.
- Oft werden verseuchte Rechner für **Denial of Service (DoS)** Attacken missbraucht. **DoS** Attacken zielen darauf ab, einen Dienst oder eine Webseite durch übermäßig häufige Anfragen zu überlasten. Wenn die Attacke nur von einer Quelle kommt, lassen sich solche Attacken sehr leicht abwehren. In Distributed Denial of Service (DDoS) Attacken werden daher infizierte Rechner missbraucht, um die Attacken zu unterstützen. DoS und DDoS Attacken können darauf zielen, das Zielsystem herunterzufahren, die Bandbreite und Speicherauslastung zu überladen oder den Dienst im Netzwerk nicht mehr auffindbar zu machen.

Ein expliziter Schadensteil kann aber auch fehlen. Aber die verschwendete Rechenzeit und der erhöhte Speicherplatz stellt ohnehin eine Payload dar.

Bedingungsteil: Sowohl die Verbreitung als auch die Schadensfunktion können von Bedingungen abhängig programmiert sein.

- Im einfachsten Fall startet der schädliche Code automatisch, ohne dass das Opfer etwas davon bemerkt.
- in einigen Fällen muss die Payload vom Opfer selbst gestartet werden. Das kann der Aufruf eines verseuchten Programms sein, das Öffnen eines E-Mail Attachments bis hin zum Phishing von persönlichen Daten.
- der Start des schädlichen Codes kann auch an Bedingungen geknüpft sein. Z.B. tritt bei einigen Viren der Schaden an einem bestimmten Datum oder bei einer bestimmten Anzahl von Aufrufen ein.

Tarnungsteil: Würmer, Trojaner und Viren versuchen sich vor der Entdeckung durch Benutzer und Virenerkennern zu schützen. Dazu verwenden Sie eine Reihe von Mechanismen.

- Sie erkennen z.B. wenn Debugger laufen oder schützen sich durch überflüssige und verwirrende (Assembler-) Codezeilen.
- Sie verbergen die Spuren einer Infektion. Dazu wird u.a. die Ausgabe von Statusmeldungen oder Log-Einträge gefälscht. Z.B. kann ein speicherresidenter Virus dem System vorgaukeln, dass der Speicher den er belegt immer noch von dem zuvor entfernten Programm stammt.
- Um der Entdeckung zu entgehen verschlüsseln manche Viren sich selbst und/oder Ihren Schadenscode. Bei der Entschlüsselung können immer die gleichen Schlüssel verwendet werden, die Schlüssel können aus einer Liste entnommen sein (oligomorph) oder die Schlüssel können unbegrenzt neu erzeugt werden (polymorph).

■ Würmer

Ein Wurm hängt sich im Gegensatz zu einem Virus nicht an ausführbare Dateien an. Er verbreitet sich dadurch, dass er sich automatisch über Netzwerke oder Mailverbindungen auf andere Rechner überträgt.

- **Netzwerk-Würmer:** In Netzwerken werden auf zufällig ausgewählten Rechnern einige Ports gescannt und wenn eine Attacke möglich ist, werden die Schwachstellen in Protokollen (z.B. IIS) oder deren Implementierung zur Verbreitung ausgenutzt. Bekannte Vertreter dieser Art sind „Lovesan/Blaser“ und „CodeRed“. Sasser nutzt einen Buffer-Overflow-Fehler in der Local Security Authority Subsystem Service (LSASS) und infiziert Rechner während einer Verbindung zum Internet.
- **E-Mail-Würmer:** Bei der Verbreitung per E-Mail kann der Wurm vorhandene E-Mail Programme (z.B. Outlook, Outlook Express) verwenden oder eine eigene SMTP-Mailengine mitbringen. Abgesehen vom entstehenden Netzwerktraffik und den erhöhten Systemressourcen können Würmer noch weitere Schadensfunktionen beinhalten. Prominente Mitglieder dieser Gruppe sind Beagle und Sober.

■ Viren

Auch Viren zielen auf ihre eigene Reproduktion und Verbreitung auf andere Computer ab. Dazu hängen sie sich an andere Dateien an oder nisten sich im Bootsektor von Datenträgern ein. Sie werden oft unbemerkt von austauschbaren

Datenträgern (wie z.B. Disketten) , über Netzwerke (auch Peer-to-Peer), per E-Mail oder aus dem Internet auf den PC eingeschleust.

Viren können an vielen unterschiedlichen Stellen im Betriebssystem ansetzen, über unterschiedlichste Kanäle wirken. Man unterscheidet folgende Gruppen:

- **Bootsektor-Viren:** Bootsektor- oder MBR-Viren (= Master Boot Record-Viren) setzen sich vor den eigentlichen Bootsektor eines Datenträgers und sorgen so dafür, dass bei einem Bootvorgang über diesen Datenträger erst der Viruscode gelesen wird und danach der Original-Bootsektor. Auf diese Weise kann sich der Virus unbemerkt in das System einnisten und wird von da ab auch beim Booten von der Harddisk mit ausgeführt. Oft bleibt der Virencode nach der Infektion im Speicher bestehen. Solche Viren nennt man speicherresident. Beim Formatieren von Disketten wird der Virus dann weitergegeben und kann sich so auch auf andere Rechner ausbreiten. Aber nicht nur bei Formatier-Vorgängen kann der Bootbereichvirus aktiv werden. So kann durch den DOS-Befehl DIR die Übertragung des Virus von einer infizierten Diskette in Gang gesetzt werden. Je nach Schadensroutine können Bootbereichviren hochgradig gefährlich oder einfach nur störend sein. Der älteste und verbreitetste Virus dieser Art trägt den Namen ‚Form‘.
- **Datei-Viren:** Viele Viren nutzen die Möglichkeit sich in ausführbaren Dateien zu verstecken. Dazu kann die Wirtsdatei entweder gelöscht/ überschrieben werden oder der Virus hängt sich an die Datei an. In letzterem Fall bleibt der ausführbare Code der Datei weiterhin funktionsfähig. Wenn die ausführbare Datei aufgerufen wird, wird zunächst der meist in Assembler geschriebene Virencode ausgeführt und danach das ursprüngliche Programm gestartet (sofern nicht gelöscht).
- **Multipartite Viren:** Diese Virengruppe ist besonders gefährlich, da ihre Vertreter sowohl den Bootsektor (bzw. Partitionstabellen) infizieren als auch ausführbare Dateien befallen.
- **Companion Viren:** Unter DOS werden COM Dateien vor gleichnamigen EXE Dateien ausgeführt. Zu den Zeiten als Rechner nur oder häufig über Kommandozeilenbefehle bedient wurden war dies ein wirkungsvoller Mechanismus um unbemerkt schädlichen Code auf einem Rechner auszuführen.
- **Makroviren:** Auch Makroviren hängen sich an Dateien an. Diese sind aber nicht selbst ausführbar. Die Makroviren sind auch nicht in Assembler, sondern in einer Makrosprache wie etwa Visual Basic geschrieben. Um die Viren auszuführen bedarf es eines Interpreters für eine Makrosprache wie sie in Word, Excel, Access und PowerPoint integriert sind. Ansonsten können die Makroviren die gleichen Mechanismen wirken wie bei Datei-Viren. Auch sie können sich tarnen, zusätzlich den Bootsektor verseuchen oder Companion-Viren erstellen.
- **Stealth-Viren:** Stealth-Viren oder Tarnkappen-Viren besitzen spezielle Schutzmechanismen, um sich einer Entdeckung durch Virensuchprogramme zu entziehen. Dazu übernehmen sie die Kontrolle über verschiedene

Systemfunktionen. Ist dieser Zustand erst einmal hergestellt, so können diese Viren beim normalen Zugriff auf Dateien oder Systembereiche nicht mehr festgestellt werden. Sie täuschen dem Virensuchprogramm einen nicht infizierten Zustand einer infizierten Datei vor. Die Tarnmechanismen von Stealth-Viren wirken erst, nachdem der Virus im Arbeitsspeicher resident geworden ist. Einige Viren benutzen Teilfunktionen von echten Stealth-Viren.

- **Polymorphe Viren:** Polymorphe Viren enthalten Mechanismen, um ihr Aussehen bei jeder Infektion zu verändern. Dazu werden Teile des Virus verschlüsselt. Die im Virus integrierte Verschlüsselungsroutine generiert dabei für jede Kopie einen neuen Schlüssel und teilweise sogar neue Verschlüsselungsroutinen. Zusätzlich können Befehlssequenzen ausgetauscht oder zufällig eingestreut werden, die nicht für das Funktionieren des Virus erforderlich sind. So können leicht Milliarden von Varianten eines Virus entstehen. Um verschlüsselte und polymorphe Viren sicher zu erkennen und zu beseitigen, reicht der Einsatz klassischer Virensignaturen häufig nicht aus. Meist müssen spezielle Programme geschrieben werden. Der Aufwand zur Analyse und zur Bereitstellung geeigneter Gegenmittel kann dabei extrem hoch sein. So sind polymorphe Viren ohne Übertreibung als die Königsklasse unter den Viren zu bezeichnen.
- **Intended Virus:** Als Intended Virus wird ein teilweise defekter Virus bezeichnet, der zwar eine Erstinfektion einer Datei vollbringt, sich von dort aus aber nicht mehr reproduzieren kann.
- **E-Mail-Viren:** E-Mail-Viren gehören zur Gruppe der sog. ‚Blended threats‘ (= vermischte Bedrohung). Solche Malware kombiniert die Eigenschaften von Trojanern, Würmern und Viren. Im Rahmen des Bubbleboy-Virus wurde bekannt, dass es möglich ist, schon über die Voransicht einer HTML-Mail einen Virus auf den PC einzuschleusen. Der gefährliche Virencode versteckt sich in HTML-Mails und nutzt eine Sicherheitslücke des Microsoft Internet Explorers. Die Gefahr dieser „Kombi-Viren“ nicht zu unterschätzen.

■ Malware im weiteren Sinn

Der Vollständigkeit halber sollen hier noch einige andere lästige und teilweise auch schädliche Kategorien erwähnt werden, die wir nicht zur Gruppe der Malware zählen.

- **Hoaxes:** Hoaxes sind angebliche Viren-Warnungen, die oftmals per E-Mail verbreitet werden. Die Empfänger werden aufgefordert die E-Mail-Warnung an Freunde und Bekannte weiterzuleiten. Meistens handelt es sich bei diesen Hinweisen allerdings nur um Panikmache.
- **Backdoor-Programme:** Viele Systemadministratoren verwenden Fernwartungsprogramme, um Rechner von seinem aktuellen Standort zu administrieren. Insbesondere bei großen Unternehmen ist dies sehr nützlich.

Üblicherweise erfolgt der Eingriff des Systemadministrators dabei mit dem Wissen und Einverständnis des PC-Users. Erst wenn diese Backdoor-Funktionen ohne Wissen des PC-Users eingesetzt werden und schädliche Aktionen ausgeführt werden wird ein Backdoorprogramm zur Malware.

- **Spyware:** Spyware zeichnet die Aktivitäten und Prozesse auf einem Rechner auf und machen sie Fremden zugänglich. Oft werden sie verwendet um das Surfverhalten zu analysieren, um passende Werbebanner einzublenden. Spyware lässt sich durch AdAware oder SpyBot-Search&Destroy entfernen. SpywareBlaster verhindert, dass Spyware auf Ihren Rechner gelangt.
- **Dialer:** Ähnlich wie Viren, Würmer und Trojaner werden Dialer oft unbemerkt auf dem Rechner installiert. Sofern die DFÜ-Verbindung über ein Modem hergestellt wird, wird dann beim nächsten Verbindungsaufbau eine teure Service-Telefonnummer verwendet. Mit dem „Gesetz zur Bekämpfung des Missbrauchs von (0)190er/(0)900er Mehrwertdiensternummern“ sind zwar seit dem 15. Aug. 2003 einige Auflagen (Preisobergrenzen, Registrierung) in Kraft getreten. Dennoch sind Dialer immer noch eine lästige Plage, die mitunter zu hohen finanziellen Schäden führen können. Mit Anti-Dialer-Programmen wie Dialer Control kann man sich vor unerwünschten Dialern schützen.
- **Spam:** Eine ebenfalls teure und lästige Plage ist das Versenden unerwünschter WerbE-Mail oder Propagandamail. Moderne Anti-Spam Programme kombinieren statische (Textanalyse, Mailserverlisten) und statistische (basierend auf Bayes Theorem) Verfahren um die unerwünschte Post zu filtern. Dazu gehört auch G DATAs AntiSpamKit.
- **Phishing:** Unter Phishing versteht man den Versuch persönliche Daten wie Loginnamen, Passwörter, Kreditkartennummern, Bankzugangsdaten etc. durch gefälschte Webseiten oder E-Mails zu erhalten. Oft wird man dazu auf gefälschte Webseiten geleitet. In den letzten Jahren hat dieses Phänomen stark zugenommen. Mehr dazu erfährt man auf www.antiphishing.org.

■ Index

A

- Abbrechen 14, 24, 34
- Abgesicherter Modus 219
- Absender-Adressen 114
- Absenderdomain 113
- Absenderfilter 106
- Account 219
- Achtung 144
- Achtung-Symbol 101
- ACHTUNG: 199
- Active Scripting 219
- Active Server Pages 219
- ActiveSync-Software 149
- ActiveX 219
- ActivX 122, 124
- Adaptiv-Modus 91
- AddOns 14
- Admin 187, 190
- Admin anmelden/abmelden: 193
- Administrator 219
- Administrator abmelden: 192
- Administrator anmelden: 192
- Administratorkonto 187
- Administratorkonto: 190
- Administratorrechte : 199
- Adressen/Domains 106, 113, 114
- Aktion, falls keine Regel zutrifft 91
- Aktionen 164, 172, 177
- Aktionen-Bereich 33, 40
- Aktiver Inhalt 219
- Aktives Profil: 148
- Aktive Tuningfunktion 148
- Aktiviert Module 149
- Aktualisieren 14, 34, 107, 108, 171
- Alle 149
- alle Dateien 50, 55
- Alle löschen 159
- Alles wiederherstellen 179
- Allgemein 144, 210
- Allgemeine Programminformationen 27
- Allgemeines 7
- alte Daten 144
- Ältere Datensicherungen löschen 172
- Ältere Datensicherungen löschen: 177
- American National Standards Institute 219
- Am Server anmelden 22, 58
- Analyse-Umfang 42
- Analyse mit rechter Maustaste 14
- andere Antivirensoftware 12
- Ändern 112, 116, 117
- Ändern eines Backup-Jobs 165, 167, 168
- Änderung der BIOS-Startreihenfolge 9
- Angewandte Technologie 181
- Angriffe 85
- Anhang 212
- Anhänge filtern 105
- Anhänge nur umbenennen 105
- Animierte Grafiken (Bilder) blocken 122, 124
- Anmelden 22, 58
- anstehenden Änderungen 149
- AntiSpam 14, 100
- AntiVireKit Unternehmenslösungen 8
- AntiVirus 14, 33
- AntiVirus Boot-CD erstellen 31
- AntiVirusLab 61
- Anwendung 80
- Anwendungen 74
- Anwendungen-Bereich 74, 80
- Anwendungen zuordnen 91
- Anwendungsdetails 95
- Anzeige 34
- Anzeige der Webfilter-Symbolleiste 122
- API 219
- Applet 219
- Application Programming Interface 219
- Archiv 219
- Archivdateien 50, 55
- Archive (monatliche Überprüfung) 42
- Archive prüfen 50, 55
- Archivierte Dateien 34
- Art 49
- Art des Archivs 172
- Art des Backups 179
- ASCII 219
- ASP 219
- AT-Befehle 219
- Attachment 219
- Attachments 105
- Auch auf Unterordner anwenden 169
- AufBlacklist 108
- auf Empfang 83
- auf Nachfrage erzeugte Regel 95
- Aufnahmeassistenten 203

- auf Viren prüfen (G DATA AntiVirus) 27
- AufWhitelist 108
- Ausdrücke 105
- Ausführen 42, 43, 148, 149, 162, 171
- Ausgeführte Änderungen 148
- Ausgehende Verbindungen 74
- Auslagerungsdatei 219
- Ausnahme 132
- Ausnahmen 50, 132
- Ausnahmetatbestände 91
- Ausnahmeverzeichnis 145
- Ausschließen von Quelldateien 172
- Auswahl 42
- Auswahlfenster 103
- Automatik 82
- automatische Typ-Erkennung 50, 55
- Automatische Updates 34, 42
- Automatische Virenprüfungen 42
- Autopilot einschalten 70
- Autosafe 199
- Autosafe: 199
- Autosafes öffnen: 192
- Autostart. 199
- Autostart bearbeiten: 199

B

- b-vertrieb@gdata.de 8
- Backdoor 255
- Backdoor-Programme 255
- Backup 14, 164, 169, 172, 179
- Backup-Job 166
- Banner blocken 122, 124
- Basis-Schutz 72
- Bayes-Methode 118
- BCC 219
- bearbeiten 167
- Bedienung der Kindersicherung 129
- Bedienung der Software 27, 33, 69
- Bedienung des Tuners 143
- Bedienung des Webfilters 120
- Bedienung von AntiSpam 100
- Bedingungsteil 255
- Beenden 14
- Beenden: 192
- Beendigung des Vertrages 164
- Beim ersten Start 22
- Beim Schreiben prüfen 34, 50
- Beim Systemstart 42

- Beliebiger Speicherort 194
- Bemerkung 112
- Benutzer 126, 129, 130, 131, 137
- Benutzer > Erlaubte Inhalte 139
- Benutzer > Verbotene Inhalte 139
- benutzerdefiniert 14, 34
- Benutzerdefinierte Einstellungen 72
- benutzerdefinierte Einstellungen 82
- Benutzer fragen 172
- Benutzerkonto 42
- Benutzerkonto: Administrator: 192
- Bericht an ausgehende Mails anhängen 61
- Beschreibung 134
- Besuchte Webseiten 122, 126
- Betreff 105
- Betreffzeile 116
- Bezahlung 212
- Bildverwaltungssoftware Picasa 149
- BIOS 219
- Bit 219
- Blacklist 108, 114, 139
- Blacklists 132
- Blind Carbon Copy 219
- Blocken getarnter URLs 124
- Blockgröße 172
- Bluetooth 219
- Bookmark 219
- Boot-CD 14
- Boot Record 219
- BootScan 12, 31, 219
- BootScan = Rootkitschutz 31
- Bootsektor 219
- Bootsektor-Viren 255
- Brennen 177
- Brenner 171
- Browser Hijacker 219
- Brute-Force Angriff 219
- Buffer Overflow 219
- Bug 219
- Bulk Mail 219
- Button 219
- Byte 219

C

- C:und EinstellungenUsersDokumente 149
- Cache 83, 219
- Carbon Copy 219
- Carrier 219

- Cascading Style Sheet 219
- CC 219
- CD-ROM prüfen 40
- CGI 219
- Client 219
- Common Gateway Interface 219
- Companion Viren 255
- Companion Virus 219
- Compiler 219
- Computernutzungsverhalten 72
- Computernutzungszeit 131
- Computernutzungszeit überwachen 137
- Cookies 126
- Cracker 219
- CRC 219
- Cross Site Scripting 219
- CSS 219
- Cyberspace 219
- Cyclic Redundancy Check 219

D

- Daemon 219
- Data Encryption Standard 219
- Datei 192
- Datei-Viren 255
- Dateien 1:1 172
- Dateiendungen 105
- Dateien in der Quarantäne 34
- Dateien komprimiert einzeln 172
- Dateien online prüfen: 40
- Dateien sichern 164
- Dateierweiterungen 105
- Dateigruppen auswählen 169
- Datei in Quarantäne verschieben 24, 50, 55
- Datei öffnen 149
- Dateischutz 146
- Dateitypbeschränkung 172
- Dateitypen 50, 55
- Dateitypen (z.B. *.dat), Zeiträume 169
- Datenkompression 172, 219
- Datenmenge 172
- Daten nachträglich brennen: 177
- Datenschutz 149, 151
- Daten sichern 166, 167, 177
- Daten sichern: 177
- Datensicherungen manuell suchen 179
- Datensicherung starten 167, 177
- Datenstand 166

- Datenverlusten 137
- Daten von Online-Backups pflegen: 177
- Daten wiederherstellen: 177
- Datum der Virensignaturen 32, 34
- dauerhafte Regel 68
- DDE-Befehle 149
- Deaktivierte Module 149
- Deaktivierung 172
- Debugger 219
- Defacement 219
- Defragmentierung 148
- Defragmentierung aller Festplatten 149
- Deinstallation 14
- Deinstallationsfunktion 149
- Denial of Service 219
- Denial of Service (DoS) 255
- DES 219
- Desinfizieren 47
- Desinfizieren (wenn nicht möglich 50, 55
- Desktopverknüpfung 189
- Desktopverknüpfungen 144
- Details 81, 95, 97, 149
- DFÜ 74
- DFÜ-Netzwerk 73
- DHCP 219
- DHTML 219
- Dialer 219, 255
- Die Bedienung der Software 129, 164, 172
- Die Bedienung von AntiSpam 100
- Dienst PKCS#11 hinzufügen 203
- Dienststatus 148
- Diese Einstellungen übernehmen 167
- Dieses Feld nicht mehr anzeigen 201
- Dieses Fenster nicht mehr anzeigen 183
- Dieses Programm speichern 172
- DirectX 219
- direkte Verbindung mit dem Internet 76
- Disassembler 219
- Disk And Execution MONitor 219
- Diskette prüfen 40
- Disk Operating System 219
- DMA-Modus 149
- DNS 219
- DNS-Anfragen 115
- DNS-WINS-Server 74
- Dokumente und Einstellungen 167, 169
- Domain 219
- Domain-Namen 106

- Domain Name System 219
- Domains 114
- Domäne 89
- DOS 219
- DoS 219, 255
- Downloadordner 144
- Drucken 14, 49
- DSL 126
- Duplex 219
- Durchsuchen 14
- Dynamic Host Configuration Protocol 219
- Dynamic HTML 219
- dynamische IP-Adresse 74

E

- E-Mail 219
- E-Mail-Adressen 106
- E-Mail-Prüfung 61
- E-Mail-Schutz 60, 109
- E-Mail-Viren 255
- E-Mail-Virenblocker (Outlook) 14
- E-Mail-Würmer 255
- E-Mail Archive prüfen 50, 55
- E-Mail Virenblocker 34
- Egress Filtering 219
- Eigene Bilder 169
- Eigene Dateien 40, 167, 169
- Eigene Filter 129, 132, 139
- Eigene Musik 169
- Eigene Videos 169
- Eigenschaften 149
- Eigenschaften: 192
- Ein Archiv 172
- Einen leeren Regelsatz erzeugen 76
- einfach / erweitert 49
- Einführung 181
- Eingebettete Mails 105
- eingehende Mails (IMAP) 109
- eingehende Mails (POP3) 109
- Eingehende Verbindungen 74
- Einloggen mit Passwort 184
- Einloggen mit Sicherheitszertifikat 185
- Ein paar Worte vorab 7
- Ein Profil hinzufügen 149
- Einstellungen 50, 55, 111
- Einstellungen: 192
- Empfangene Mails auf Viren prüfen 61
- Engines benutzen 50, 55, 61

- Entf 49
- entfernen 167
- Entfernte Adresse 80
- Entfernter Port 80
- Erkennungsteil 255
- Erlaubte Inhalte 134
- Erlaubter Inhalte 131
- Erstellen. 200
- Erstellen eines neuen Backup-Jobs 167
- Erster Programmstart 183
- Erste Schritte 68
- Erweitert 22, 34, 58
- Ethernet 219
- Exploit 219
- Export-Textdatei 113, 116, 117
- externen Festplatten 171
- Extras 61, 192
- Extras > Ordner auf Viren überprüfen 60

F

- FAQ 219
- FAT 219
- Fehlermeldung 141
- Fertig stellen 14
- Festlegen von Verhaltensmaßregeln 9
- Festplatte 149
- Festplatten 149, 171
- File Transfer Protocol 219
- Filter 112, 118, 132, 134
- Filter-Bereich 103
- Filter-Update 129
- Firefox-Browser 144
- Firewall 14, 58, 68, 219
- Firewall-Alarm 68, 76, 95
- Firewall-Notaus aktivieren / aufheben 28
- Firewall aktiv, auf diesem Netzwerk 74
- Firewall ausschalten 28
- Firewall deaktiviert 72, 82
- Flame 219
- Flash blocken 124
- Flash blockenSkip Intro 122
- Flooding 219
- Fortsetzen 24
- Fragezeichen-Symbol 50, 146
- fragmentiert 149
- FTP 91, 171, 219
- FTP-Server 164, 172, 219
- FTP-Speicherplatz 164

G

Gateway 219
G DATA AntiSpam 7
G DATA AntiVirus 7, 27
G DATA FTP-Server 172
G DATA InternetSecurity starten 28
G DATA Kindersicherung 7
G DATA Personal Firewall 7
G DATA ServiceCenter 8
G DATA Shredder 14
G DATA WebFilter / Datenshredder 7
Gefährliche Anhänge filtern 101
Gemeinsame Nutzung: 199
Geringe Sicherheit 34
Geschütztes Verzeichnis TopSecret 194
Gespeicherte Formulardaten 126
getarnte URLs 124
Gewährleistung 212
GIF 122, 124
Glossar 219
Gopher 219
Größenbegrenzung für Downloads 120, 141

H

Haftung 212
Häkchen 32, 34, 71, 101
Häkchensymbol 101
Hauptfenster 190
HBCI 219
Header 105, 219
Helkern 85
Heuristik 50, 55, 219
High Tech vollautomatisch 7
Hijacker 219
Hilfe 27, 34, 70, 147, 192
Hilfe-Bereich 100, 120, 129, 164
Hilfe: 193
Hinzuf. 169
Hinzufügen 116, 117, 134, 145, 146, 209
History 126
Hoax 219
Hoaxes 255
Hoch (Kurze Laufzeit) 55
Höchste Sicherheit 34, 72, 82
Hohe Sicherheit 34, 72, 82
Hohe Spamwahrscheinlichkeit 112
Hop 219
Host 219

Hostnamen 66
HOSTS-Datei 66
HTML 219
HTML-Mails 105
HTML-Scripte deaktivieren 104
HTML-Skripte deaktivieren“ 101
HTML-Text 105
HTTP 219
HTTP-Protokoll 120, 124
HTTP-Webinhalte 141
HTTPS 219
Hub 219
Hyperlink 219
Hypertext 219
HyperText Markup Language 219
HyperText Transfer Protocol 219
HyperText Transfer Protocol Secure 219

I

IANA 219
ICMP 219
ICMP-Details 91
ICMP Flood 85
ICP 219
IE 219
IMAP 219
Im Fall einer Infektion 47, 50, 55, 61
Im gesamten Text 132
Immer erlauben 95
Immer verweigern 95
Import-Export-Textdatei 114
Import-Listen von Schlüsselwörtern 117
Import-Notepad 113, 116
inaktiv 148
Infizierte Archive 50, 55
Infizierte Datei löschen 24
Info-Box 68
Informationen zu Viren 9
Inhaltsfilter 105, 118
Inklusive Online-Speicherplatz (1 GB) 164
Installation 12
Installationsvorbereitung 12
Installationsvorgang 14
Installieren 14
Intended Virus 255
Internet 144, 219
Internet-Ambulanz 47
Internet-Dienst zuordnen 91

- Internet-Einstellungen 58, 61
- Internet-Update 8, 58
- Internet Ambulanz 47
- Internet Assigned Numbers Authority 219
- Internet Cache Protocol 219
- Internet Control Message Protocol 219
- Internet Explorer 120, 122, 149, 219
- Internetinhalte (HTTP) verarbeiten 120, 141
- Internet Message Access Protokoll 219
- Internetnutzungszeit 131
- Internetnutzungszeit überwachen 135
- Internetrecherchen 149
- Internet Relay Chat 219
- Internet Update 22
- Internetverbindungsaufbau 42, 43
- Internetverbindungsfreigabe 74, 89
- In the wild 219
- IP-Adresse 74, 219
- IP-Adressen 115
- IP-Adressraum 91
- IPX/SPX 219
- IRC 219
- ISDN 219
- ISP 219
- ITW 219

J

- JA 199
- Java 219
- JavaApplets 122, 124
- JavaScript 122, 124, 219
- JavaScript Style Sheet 219
- Jetzt starten 160
- Job 42
- JPEG 219
- JPG 219
- JScript 219
- JScript blocken 122, 124
- JSSS 219

K

- Kaltstart 219
- Karteikarten 33, 69
- KBit 219
- KByte 219
- Keine 149
- Kein Spam 100, 108
- Kermit 219

- Keylogger 219
- Kindersicherung 14, 129
- Kommentar 91, 177
- Kompression 172, 219
- Komprimierung 219
- Konfiguration 148, 149, 161, 162
- konfigurieren 72
- Kontextmenü 68, 219
- Konvertierung 219
- Kundendaten 22, 58

L

- Label auf dem Medium 172
- LAN 74, 219
- Land 85
- LASE 219
- Laufzeitfehler 219
- Leistung 149, 153
- Letzte Aktion 80
- Letzte Analyse des Rechners 34
- Letzte Ausführung 148
- Letzte Modemverbindungen 126
- Limited Area Search Engine 219
- Lineare Verbindung 219
- Link 219
- Link zum Angebot 134
- Liste gemeinsam verwendeter Dateien 149
- LiveScript 219
- Lizenzvereinbarungen 121
- Local Area Connection 73
- Local Area Network 219
- Log-Datei 180
- Log-Dateien 162
- Login 219
- Logoff 219
- Lokale Festplatten 42
- Lokaler Port 80
- Lösche Firefox Cache: 149
- Lösche Firefox Cookies: 149
- Lösche Firefox Verlaufsprotokoll: 149
- Lösche Internet Explorer Cache: 149
- Lösche Internet Explorer Cookies: 149
- Löschen: 193
- Lösche Netscape Cache: 149
- Lösche Netscape Cookies: 149
- Lösche Netscape Verlaufsprotokoll: 149
- Lösche Opera Cache: 149
- Lösche Opera Verlaufsprotokoll: 149

Lösche Ordner mit temporären Dateien: 149
Lösche ungültige Autostart-Befehle 149
Lösche ungültige Browser-Hilfsobjekte: 149
Lösche ungültige Datei-Referenzen: 149
Lösche ungültige Shell-Befehle: 149
Lösche ungültige Treiberinformationen: 149
Lösche ungültige Uninstall-Referenzen: 149
Lovesan 85

M

MAC-Adresse 219
Mac OS 219
Mail-Anhänge 105
Mailbomb 219
Mailbox 219
Mailingliste 219
Mail in Ordner verschieben 105, 106, 112
Mailstatus 100
Mails vor dem Senden prüfen 61
Mailtext 105, 117, 118
Mail zurückweisen 105, 106, 112
Makros 105
Makroviren 255
Malware im weiteren Sinn 255
MAPI 219
MARS 182
Max. Datenmenge je Medium 172
MB 219
MBit 219
MByte 219
Media Access Control 219
MegaByte 219
Mehrfachlizenzen 164
Meldung anzeigen wenn... 141
Meldung im Text der Mail einfügen 105
Meldung in Text 105, 106
Menüleiste 34, 69, 70, 192
Message 219
Meta 132
Methoden der Authentifizierung 181
Microsoft Office 144, 149
Microsoft Outlook 105, 106, 109
Microsoft PictureIt!/Digital Image Pro 149
MIME 219
Miniaturansichten 149
Mittlere Sicherheit 34
mm 135, 137
MMX 219

mobilen Safe 188
Mobilen Safe erstellen 192, 203
Mobilen Safe erstellen: 190
Mobilen Safe öffnen 204
Mobiler Safe 203
Modem 219
Modemverbindung 126
Modus 85
MPEG 219
MultiMedia eXtensions 219
Multipartite Viren 255
Multipurpose Internet Mail Extensions 219

N

Nach der Datensicherung 172
Nach der Datensicherung testen 172
Nachfrage 83
Nächstes Vollbackup 166
Name 91, 112, 161
NameBemerkung 103
Name des Jobs 179
Name und Kommentar 177
NAT 219
Nebenabreden 212
Negativliste 169
NetBIOS 89
Netiquette 219
Network Address Translation 219
Netzlaufwerke 171
Netzwerk 80, 219
Netzwerk-Info 74
Netzwerk-Verlauf 126
Netzwerk-Würmer 255
Netzwerkaktivitäten 68
Netzwerke 73
Netzwerke-Bereich 74
Netzwerkzugriffe prüfen 50
Netzzugriffe 91
Neu 76, 127, 132, 134, 139, 167, 194
Neu: 193
Neuen Benutzer anlegen 131
Neuer Benutzer 131
Neuer Regelsatz 76
Neue Systemprüfung 160
Neue Virenprüfung 42
neue Zugangsmethode 186
Newsgroup 219
NIC 219

- nicht löschen 172
- nicht vertrauenswürdige Netzwerke 76
- Niedrig (Lange Laufzeit) 55
- Niedrige Sicherheit 72, 82
- NNTP 219
- Normale Sicherheit 72, 82
- Notaus 28, 70
- Notaus aktivieren 70
- Notepad 117
- NullSession 219
- Nur einzelne Dateien wiederherstellen 179
- nur Programmdateien 50, 55
- Nur protokollieren 24
- nur Testen 179
- Nur vollständige Wörter suchen 116, 117

O

- OCX 219
- ODBC 219
- ORDER 105
- Office-Aktualisierungen 144
- Offline 219
- Offline-Reader 219
- Öffne im Modus „Nur lesen“: 199
- Öffnen 49, 162
- Öffnen/Schließen: 193
- Öffnen als Wechselmedium: TopSecret 199
- Öffnen Dialog 149
- Öffnen mit 149
- Öffnen und Schließen von Safes 201
- OK 149, 169
- Online 219
- Online-Speicherplatz 164
- Online-Spiele 91
- Operatoren 105
- Optionen-Bereich 120
- Optionen > E-Mail-Prüfung 34
- Optionen > E-Mail-Schutz 34
- Optionen > Einstellungen 109, 149
- Optionen > Internet-Update 42, 58
- Optionen > Nachfrage > Regel erstellen 95
- Optionen > Regelsätze 76
- Optionen > Virenprüfung 34, 42, 47, 49
- Optionen > Wächter 34
- Ordner auf Viren prüfen 61
- Ordnername 105, 106, 112
- Ordnerschutz 145
- Original-Software verwenden 9

- Ort der Suche 132
- OSI Schichtenmodell 219
- OutbreakShield 34, 61
- Outlook 60, 111
- Outlook Express 105, 106

P

- P2P 219
- Packeting 219
- Packet INternet Grouper 219
- Pageview 219
- Paket-Info 95, 99
- PAP 219
- Papierkorb 149
- Password Authentication Protocol 219
- Passwort 131, 172
- Passwortgeschützte Archive 34
- Patch 219
- Pause 24
- Payload 219
- Payload-Trigger 219
- PDC 219
- PDF 219
- PE Datei 219
- Peer 219
- Peer-to-Peer 219
- Perl 219
- per Nachfrage generiert 91
- Personal Identification Number 219
- persönliche Informationen 126
- PGP 219
- Phishing 219, 255
- Phishing-Websites 66
- Phishingseiten blocken 122, 124
- PIN 219
- Ping 219
- Ping of Death 85
- PIO-Modus 149
- PKCS#11 203
- PNG 122, 124
- Pocket PC 149
- Point to Point Protocol 219
- Polymorphe Viren 219, 255
- Pop-Up 219
- POP3 111, 219
- POP3/IMAP-basierten E-Mail-Postfächer 109
- Popup blocken 122, 124
- Popup überwachen 122, 124

- Port 60, 89, 109, 219
- Portable Document Format 219
- Portablesafe erstellen 181
- Port Scans 85
- Positivliste 169
- Post-Office Protocol 3 219
- Posting 219
- PostScript 219
- PPP 219
- Precise Biometrics 181, 186
- Prefix in Betreffzeile 105, 106
- Pretty Good Privacy 219
- Primary Domain Controller 219
- Printer Access Protocol 219
- Priorität Scanner 55
- Private Key 219
- pro Anwendung 83
- Pro Anwendung, falls min. ___ Nachfragen anstehen 83
- Profi-Dialog 76
- Profi-Dialog verwenden 91
- Profi-Einstellungen 119
- Profil 161
- Profil definieren 149, 159
- Programmaufbau 188
- Programmbereiche > Aktionen-Bereich 42
- Programmbereiche > Netzwerk-Bereich 73
- Programmbereiche > Protokolle-Bereich 42
- Programmbereiche > Zeitplan-Bereich 34
- Programmdateien 14
- Programmeinstellungen und Protokolle 14
- pro Protokoll/Port/Anwendung 83
- pro Protokoll/Port/Anwendung. 83
- Protokoll 80, 89, 91, 129, 140, 141, 219
- Protokoll anfertigen 42, 55
- Protokolldateien 162
- Protokolle 144, 162, 164, 180
- Protokolle-Bereich 33, 49
- Protokolle löschen 140, 141
- Provider 219
- Proxy 219
- Proxyserver 58, 61
- Public Key 219
- Pufferüberlauf 219
- Pulswahlverfahren 219

Q

- Quarantäne-Bereich 33, 47

- Quellcode 219

- Quicktime 219

R

- RADIUS 219

- RAID 219

- RAID 0 219

- RAID 1 219

- RAID 4 219

- RAID 5 219

- Rang 91

- Raubkopie 219

- RBLs (Realtime Blacklists) 115

- RC6 182

- Re-Mailer 219

- Reaktion 105, 106, 107, 112

- Realtime Blacklists 115

- Rechnerabsturz 126

- Rechner prüfen 40

- Rechner wöchentlich auf Viren prüfen 14

- rechten Maustaste 68

- Red Book 219

- Redundant Array of Inexpensive Disks 219

- Regel-Assistent 76

- Regel-Assistenten 89, 91

- Regel-Assistenten verwenden 89

- Regel aktiv 91

- Regel bearbeiten 91

- Regel erstellen 83

- Regeln 91

- Regeln erstellen 89

- Regeln erstellen > Firewall-Alarm 76

- Regelsatz 74

- Regelsatz bearbeiten 74

- Regelsätze 95

- Regelsätze-Bereich 74, 76

- Regelsätze erstellen 76

- Regelsatz für zu blockierende Netzwerke 76

- Regelsatzname 76

- Registriernummer 8, 22, 58

- Registry 219

- Remote Dial In User Service 219

- Reply 219

- Reproduktionsteil 255

- Request for Comments 219

- RFC 219

- RFID 219

- RFID Tag 219

Rhythmus 162
Rich Text Format 219
Richtung / Verbindungsrichtung 91
Rijndael 182
RIP 219
RIPE 219
Robot 219
Router 219
Routing 219
Routing Information Protocol 219
RTF 219
Rückgängig 144, 159
Rückkanal-Technik 91
Runtime error 219

S

S/MIME 219
Safe an ausgewähltem Ort öffnen 194
Safeeigenschaften 210
Safeeigenschaften: 190
Safe erstellen 194
Safe Fenster 193
Safe hinzufügen 190, 209
Safe hinzufügen: 192
Safeinformation hinzufügen: 190
Safe Konfiguration 200
Safe löschen: 192
Safe mit Datenträger verknüpfen 203
Safe neu: 192
Safe öffnen/schließen: 192
Safes 194
Safe schließen 201
Safe verschieben 208
Safe verschieben: 190, 192
Safezugang 210
Safezugang - Berechtigung 199
Safezugang - Einstellung 197
Safezugang und Berechtigung 199
Scannen 95
Schadensteil 255
Schätzen der Datenmenge 172
Schließen 22, 24, 34, 58, 149
Schlüsselwörter 105
Schlüsselwörter (Betreff) 116
Schlüsselwörter (Mailtext) 117
schwarze Listen 115
SD-Karten 171
SDK 219

Security-Symbol 14, 28, 68
SecurityCenter 32
Sehr hohe Spamwahrscheinlichkeit 112
selbstlernend 68
selbstlernenden Filter 118
Semikolon 106
Serpent 182
Server-Anwendungen 74
Serverportnummer 60, 109
ServiceCenter 164
SET 219
setup.exe 14
Short Messages Service 219
Shredder 28
Shreddern 28
Sicherheit 72, 149, 157
Sicherheit / Performance 34
Sicherheitsabfrage 144
Sicherheit/Sicherheitsvarianten 72
Sicherheitsstufe 82
Sicherung auf CD/DVD 172
Skip Intro 124
Smb Die; 85
Software-Update 40
Software Development Kit 219
Spam 100, 108, 115, 219, 255
Spam-Filter 100, 101, 103, 108, 112
Spam-OutbreakShield 101
Spamerkennung 119
Spamprüfung für Microsoft Outlook 14
Spamwahrscheinlichkeit 115, 116, 117, 118
Speichern 149
speichern 186
Speichern auf Wechseldatenträgern 181
Speichern unter 49
Speicher und Autostart 40
Spezielle Ordner suchen 169
Spezifische Spuren löschen 122
Spitzentechnologie 7
Sprachenfilter 107
Spuren 120
Spurenlöscher 120, 122, 126
Spyware 219, 255
Stammdaten 139
Standard 60, 109
Standardgateway 74
Standardoptionen benutzen 172
Startzeit 49

- Statistik 28, 34, 68, 100, 107
- Status 49, 66, 80, 101, 148, 164, 166
- Status-Bereich 33, 34, 66, 71
- Stealth-Modus 91
- Stealth-Viren 255
- Sternchen-Symbol 50, 146
- Structured Query Language 219
- Subnetzmaske 74
- Suchbereich 105
- Sucheinstellungen 126
- Suchkriterium 105
- Suchvorgänge 149
- Suffix 105
- Surfverhalten 120
- Symbolleiste 122
- SYN Flood 85
- Systemanwendungen anzeigen 80
- Systembereiche prüfen 55
- Systemdatei 172
- Systemdateien (Dateiattribut) 172
- Systemnachrichten 74
- Systemschutz 66
- Systemvoraussetzungen 11

T

- Tabbed Browsing 219
- Tabelleninhalte abfragen 118
- Tabellen zurücksetzen 118
- Tage/hh 135, 137
- Täglich 42, 162
- Tarnungsteil 255
- Taskleiste 28, 219
- TCP/IP-Netzwerk 74, 89
- temporär 172
- Temporäre Dateien 145
- Temporäre Dateien (Dateiattribut) 172
- Temporäre Internetdateien 126
- Temporäre Nutzerdateien 126
- Temporär erlauben 95
- Temporär verweigern 95
- Temporärverzeichnis mit Dateien 172
- Terminal 219
- Testen... 129
- Testlauf 149
- Test nach dem Sichern 172
- Text-Mails 105
- Thread-Priorität 172
- Thumbs.db 172

- Tipps zur Deinstallation 14
- Tipps zur Virenprophylaxe 9
- Titel 49, 132
- TLD 219
- Toolbars 149
- Top Level Domain 219
- TopSecret - Hilfe: 192
- TopSecret - Information: 192
- TopSecret. 192
- TopSecret starten 187, 189, 190
- Treiberinformationsdateien 149
- Trojaner 219, 255
- Trojanisches Pferd 219
- Tuner 14, 143
- Twofish 182

U

- UDP Flood 85
- Umfassende Sicherheit 7
- Umschalten 149
- Unbekannte Server-Anwendungen 74
- unbekannte Server-Anwendungen 74
- Unbekannte Serveranwendungen 83
- UND 105
- Ungelesene Nachrichten 74
- Ungeschützte Netzwerke 83
- Unterverzeichnisse durchsuchen 209
- Update-Bereich 120
- Updates 149
- Updates & PremiumSupport 7
- Updates / Upgrades 7
- Updates durchführen 22
- URL 132, 219
- URLs 124
- USB-Sticks 171

V

- VBScript blocken 122, 124
- Verbindungen 74
- Verbindungen-Bereich 81
- Verbindungsanforderung 83
- Verbindungsanfragen 83
- Verbindungsdetails 80
- Verbindungsrichtung 89
- Verbotene Inhalte 132
- Verbotener Inhalte 131
- Verbotsschild 32, 34, 71, 101
- Verlauf 126

- Verlauf angemeldeter Nutzer 126
- Verlauf ausgeführter Programme 126
- Verlauf gesuchter Objekte 126
- Verlaufslisten 149
- Verschieben 208
- Verschlüsselungsalgorithmus 182
- Versionsinformation 61
- Versionsprüfung 58
- Vertragsgegenstand 212
- vertrauenswürdige Netzwerke 76
- Verzeichnisse/Dateien prüfen 40
- Viren 255
- Viren-Update 28, 40
- Virengeschichte 213
- Vireninformation 24
- Virenkategorien 255
- Virenlexikon 34
- Virenprüfung 24, 42, 55
- Virenprüfung starten 24
- Virensignaturen 42
- Virenüberprüfung 172
- Virenupdate stündlich laden 14
- Virenwächter 14, 34
- Virus News 61
- Visit 219
- Visual Basic Script 122, 124
- VNC 219
- vollständig 14
- vor der Installation 12
- Voreingestellte Regel 91

W

- W3C 219
- Wächter 50
- Wächter Ausnahmen 50
- Wächter einschalten / ausschalten 28
- Wächtereinstellungen 34
- Wächterstatus 50
- Wächtersymbol 14
- Was ist eine BootCD? 12
- Web 141
- Web-Filter 120
- WebFilter 122, 124
- Webfilter 14, 120, 124
- Websites 120
- Wechselmedien 171
- WEITER 194
- Weiter 14, 168, 177, 179, 203

- Weiter, 203
- Weitere 66
- Weitere Filter 100, 103
- Werbebanner 122, 124
- Werkzeugleiste 193
- Whitelist 108, 113, 120, 127, 139
- Whitelists 134
- Wiederherstellen 164, 177, 179
- Wiederherstellungsdaten 144
- Wiederherstellungspunkt 159
- Wiederherstellung starten 179
- Wildcard 169
- Windows-Benutzerkonto 131
- Windows-Updates 144, 149
- Windows Explorer 149
- Windows Kontextmenü 27
- Wochentage 42, 43, 162, 171
- Wollen sie das erlauben 95
- Würmer 255

Z

- Zeiten sperren 135, 137
- Zeitersparnis 55
- Zeitfenster 91
- Zeit freigeben 135, 137
- Zeitmarke 80
- Zeitplan 34, 148, 149, 160
- Zeitplan-Bereich 33, 42
- Zeitplanung 42, 148, 162, 171
- Zeitpunkt 42, 43, 162, 171
- Zeitraum 135, 137
- Zeiträume 135, 137
- Zeit sperren 135, 137
- Zielordner 14, 171
- zu blockierende Netzwerke 76
- Zugang mit Sicherheitszertifikat 203
- Zugriff 80, 91
- Zugriff verweigert 34
- Zuletzt verwendete Dateien 126
- Zuletzt verwendete Dokumente 149
- Zurück 200
- Zurückbewegen 47
- Zurücksetzen 107
- Zusätzliche Dateien 172
- Zu sichernde Dateien und Ordner 169